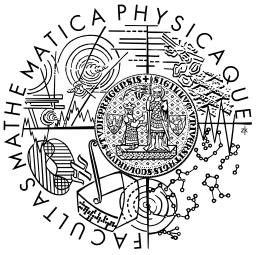


MATEMATICKO-FYZIKÁLNÍ FAKULTA
Univerzita Karlova

DIPLOMOVÁ PRÁCA

Bc. Marek Bajtoš

Asymptotika v maximálne neasociatívnych kvázigrupách

Katedra algebry

Vedúci diplomovej práce:	prof. RNDr. Aleš Drápal, CSc., DSc.
Študijný program:	Matematika
Študijný odbor:	Matematika pre informačné technológie

Praha 2021

Prehlasujem, že som túto diplomovú prácu vypracoval samostatne a výhradne s použitím citovaných prameňov, literatúry a ďalších odborných zdrojov. Táto práca nebola využitá k získaniu iného alebo rovnakého titulu.

Beriem na vedomie, že sa na moju prácu vzťahujú práva a povinnosti vyplývajúce zo zákona č. 121/2000 Sb., autorského zákona v platnom znení, najmä skutočnosť, že Univerzita Karlova má právo na uzavretie licenčnej zmluvy o využití tejto práce ako školského diela podľa §60 odst. 1 autorského zákona.

V Prahe dňa 21.5.2021

Bajtoš

Podpis autora

Na tomto mieste by som chcel vyjadriť svoje poďakovanie vedúcemu tejto práce profesorovi Alešovi Drápalovi, za jeho cenné rady, značnú trpezlivosť a neustálu pripravenosť pomôcť vo chvíľach, keď nejde všetko podľa plánu. Jeho pomoc bola neoddeliteľnou súčasťou tvorby tejto práce, za čo mu patrí veľké poďakovanie.

Tiež by som chcel z celého srdca poďakovať svojej milovanej manželke Patrícií a synovi Marekovi za maximálnu podporu a za to, že tu boli pre mňa vždy, keď mi už dochádzali sily a dokázali ma nakopnúť a dodať pozitívnu energiu, aby som túto prácu dotiahol do úspešného konca.

Názov práce: Asymptotika v maximálne neasociatívnych kvázigrupách

Autor: Bc. Marek Bajtoš

Katedra: Katedra algebry

Vedúci diplomovej práce: prof. RNDr. Aleš Drápal, CSc., DSc., Katedra algebry

Abstrakt: Táto práca nadväzuje na výsledky práce A. Drápal a I. M. Wanless, On the number of quadratic orthomorphisms that produce maximally nonassociative quasigroups. Práca sa zaoberala hustotou maximálne neasociativných kvázigrup určitej konštrukcie. Pri výpočtoch sa však kvôli obmädzujúcim podmienkam museli určité prípady zanedbať. Preskúmanie týchto prípadov je predmetom tejto práce. Ukázalo sa, že asymptotické chovanie v obecnom prípade ako v uvedenom článku sa líši od chovania v prípadoch skúmaných v našej práci. Okrem samotných výpočtov práca obsahuje teoretický úvod s vysvetlením konštrukcií využitých v predchádzajúcom článku, ako aj vlastnú teóriu potrebnú pre naše výpočty. Naše výsledky sme navyše experimentálne overovali.

Kľúčové slová: kvázigrupa, asociatívna trojica, maximálne neasociatívna kvázigrupa, kvadratický ortomorfizmus, Weilov odhad

Title: Asymptotics in maximally nonassociative quasigroups

Author: Bc. Marek Bajtoš

Department: Department of Algebra

Supervisor: prof. RNDr. Aleš Drápal, CSc., DSc., Department of Algebra

Abstract: This thesis follows up the results of article A. Drápal a I. M. Wanless, On the number of quadratic orthomorphisms that produce maximally nonassociative quasigroups. This paper dealt with the density of maximally non-associative quasigroups of a certain construction. However, certain cases had to be neglected in the calculations due to restrictive conditions. The examination of these cases is the subject of this work. It turned out that the asymptotic behavior in the general case as in the article differs from the behavior in cases examined in our work. In addition to the calculations themselves, the work contains a theoretical introduction with an explanation of the constructions used in the previous article, as well as our own theory necessary for our calculations. In addition, we experimentally verified our results.

Keywords: quasigroup, associative triple, maximally nonassociative quasigroup, quadratic orthomorphism, Weil bound

Obsah

Úvod

V oblasti kryptografie sa dnes využívajú rôzne typy matematických štruktúr, ktoré napríklad umožňujú vytvárať bezpečné šifrovacie algoritmy a hašovacie funkcie. Medzi také matematické štruktúry, ktorým sa v dnešnej dobe venuje pozornosť, sa určite radí aj kvázigrupa. Dnes už existujú viaceré návrhy kryptografických primitivov využívajúcich vlastnosti kvázigrup. Napríklad v článku [1] je uvedený súhrn možností využitia kvázigrupy v kryptografii, kde sú medzi inými uvedené aj možnosti využitia v hašovacích funkciách alebo v prúdových šifrách.

Aby sme uviedli motiváciu našej práce, môžeme ešte spomenúť článok [2], ktorý rovnako ako [1] uvádza, že sa ukazuje byť výhodne pri návrhoch kryptografických systémov použiť neasociatívne štruktúry, ako napríklad kvázigrupy. Bolo však potrebné dokázať, že existujú kvázigrupy, ktoré splňujú vlastnosť, ktorú budeme označovať ako maximálna neasociativita, čo znamená, že jediná trojica (a, b, c), ktorá je v kvázigrupe asociatívna je prípad, keď $a = b = c$. Táto existencia bola dokázaná v článku [3], ale existenciu takej kvázigrupy sa nepodarilo dokázať pre všetky rády.

Na článok [3] plynulo nadviazal článok [4], ktorý sa zaoberal hustotou maximálne neasociatívnych kvázigrup daného rádu. V tejto práci bude našou úlohou nadviazať na článok [4] a určiť hustotu týchto kvázigrup pre špeciálne prípady, ktoré boli pri určovani hustoty v predchádzajúcom článku zanedbané. Ide konkrétne o prípady, ktoré nejakým spôsobom narušovali predpoklady pri odhadoch hustoty v obecnom prípade. Náš predpoklad je, že by tieto špeciálne prípady mohli dopadnúť tak, že hustota maximálne neasociatívnych kvázigrup bude výrazne odlišná od tej, ktorá bola dokázaná v zdrojovom článku. Toto porovnanie si teda necháme do záveru našej práce, kde zhodnotíme, či bol náš predpoklad správny.

Práca je štrukturovaná do 5 hlavných kapitol. Úvodná Kapitola 1 je venovaná prevažne uvedeniu do problematiky, ktoré zahrnuje definície používaných pojmov a tiež tvrdení z článkov, na ktoré sa v našej práci snažíme nadviazať. V záujme schopnosti čitateľa porozumieť uvádzaným tvrdeniam a pojmom, sú niektoré tvrdenia uvedené aj s dôkazom. Táto kapitola je zakončená uvedením spomenutých špeciálnych situácií (sekcia 1.5), ktorých preskúmanie je hlavným cieľom práce. Okrem iného tam zdôvodníme, prečo sú práve tieto sitácie hodné preskúmania a tiež ako z pôvodne vyžadovaných 12 špeciálnych prípadov si vystačíme s preskúmaním iba 3.

Nasledujú 3 kapitoly, ktoré sú svojou štruktúrou podobné a každá z nich je venovaná jednému špeciálnemu prípadu. Každá z týchto kapitol najprv uvedie 2 kľúčové tvrdenia z článku [4] v podobe, ktorá odpovedá uvedenej špeciálnej situácií. Tieto tvrdenia sa vo zvyšku kapitoly využijú na odhad hustoty maximálne neasociatívnych kvázigrup. Tieto kapitoly teda obsahujú hlavný prínos práce.

Záverečná Kapitola 5 dopĺňa predchádzajúci výklad o algoritmy, ktoré boli úspešne použité k overeniu správnosti získaných výsledkov. Vďaka tomu práca získala okrem teoretického a výpočtového aj implementačný rozmer. Dodajme, že samotná implementácia je uvedená ako elektronická príloha tejto práce a niektoré výsledky výpočtov sa dajú nájsť na konci textu v prílohe.

1. Základné pojmy a tvrdenia

Ako sme už v úvode spomenuli, táto práca nadväzuje na články [3] a [4], preto venujeme prvú kapitolu uvedeniu základných pojmov a tvrdení z týchto prác, o ktoré sa budeme opierať vo zvyšku našej práce. Okrem pojmov a tvrdení vychádzajúcich z týchto článkov budeme potrebovať aj určité vlastnosti konečných telies, ktoré uvedieme v nasledujúcej podkapitole.

1.1 O štvorcoch v telese

Teleso rádu q, kde q je mocnina nepárneho prvočísla, budeme označovať $\mathbb{F}_q$.

Definícia 1.1. ***Štvorec*** *je také $u \in \mathbb{F}_q$, že existuje $v \in \mathbb{F}_q$ tak, že $u = v^2$. Ak také v neexistuje, tak povieme, že u* ***nie je štvorec*** *alebo že je* ***neštvorec****.*

Pre zjednodušenie zápisu, či je nejaký prvok $\mathbb{F}_q$ štvorec alebo nie, budeme používať kvadratický charakter.

Definícia 1.2. ***Kvadratický charakter*** *χ je zobrazenie*

$$\chi : \mathbb{F}_q \to \{\pm 1, 0\}$$

definované pre $u \in \mathbb{F}_q$ ako

$$\chi(u) = \begin{cases} 0 & \text{ak } u = 0, \\ 1 & \text{ak je } u \text{ nenulový štvorec}, \\ -1 & \text{ak nie je } u \text{ štvorec}. \end{cases}$$

Vlastnosť kvadratického charakteru, ktorú budeme ďalej vo veľkej miere využívať je, že pre $u, v \in \mathbb{F}_q$ platí $\chi(u \cdot v) = \chi(u) \cdot \chi(v)$.

V ďalších častiach práce budeme okrem iného určovať počet štvorcov určitého tvaru v telese. Najprv teda uvedieme klasický výsledok a následne ešte jedno tvrdenie z článku [5] zaoberajúce sa počtom štvorcov istého tvaru.

Veta 1.3. *Nech $\mathbb{F}_q$ je konečné teleso nepárneho rádu q. Potom je v tomto telese presne $(q-1)/2$ nenulových štvorcov a $(q-1)/2$ neštvorcov.*

Dôkaz. Stačí si všimnúť, že $\varphi : \mathbb{F}_q^* \to \mathbb{F}_q^*$, $\varphi(u) = u^2$ je grupový homomorfizmus. Ak je $q \neq 2$, potom je jadro tohto homomorfizmu $\mathrm{Ker}(\varphi) = \{-1, +1\}$. Potom už vďaka 1. vete o izomorfizme grup platí $\left|\mathbb{F}_q^*/Ker(\varphi)\right| = |Im(\varphi)| = (q-1)/2$. □

Veta 1.4. *Nech q je mocnina nepárneho prvočísla.*

- *Ak je q tvaru $q = 4k-1$, potom je v $\mathbb{F}_q$ práve $2k$ štvorcov $r_1, \ldots, r_{2k}$ (vrátane nuly) a $2k-1$ neštvorcov $s_1, \ldots, s_{2k-1}$.*

  Pre $a \in \mathbb{F}_q$ navyše platí, že k čísel z množiny $\{r_1 + a, \ldots, r_{2k} + a\}$ sú štvorce (vrátane nuly) a pre zvyšných k čísel platí, že nie sú štvorce. Pre toto a tiež platí, že k čísel z množiny $\{s_1 + a, \ldots, s_{2k-1} + a\}$ sú štvorce (vrátane nuly) a pre zvyšných $k-1$ čísel platí, že nie sú štvorce.

- *Ak je q tvaru $q = 4k+1$ platí, že v $\mathbb{F}_q$ je práve $2k+1$ štvorcov $r_1, \ldots, r_{2k+1}$ (vrátane nuly) a $2k$ neštvorcov $s_1, \ldots, s_{2k}$.*

  Pre $a \in \mathbb{F}_q$ navyše platí, že ak je a štvorec, tak $k+1$ čísel z množiny $\{r_1 + a, \ldots, r_{2k+1} + a\}$ sú štvorce (vrátane nuly), pre a neštvorec je to k čísel, zvyšné čísla nie sú štvorce. Pre toto a tiež platí, že ak je a štvorec, potom k čísel z množiny $\{s_1 + a, \ldots, s_{2k} + a\}$ sú štvorce (vrátane nuly), pre a neštvorec je to $k+1$, zvyšné čísla nie sú štvorce.

Dôkaz. Pôvodne bola v [5] táto veta formulovaná iba pre prvočísla. Dôkaz tejto vety, ako je uvedený v [5], však prejde bez zmeny pre obecné konečné teleso nepárneho rádu.

□

Ak si pre pevne zvolený prvok $a \in \mathbb{F}_q$ položíme otázku, a akou pravdepodobnosťou platí, že pre $u \in \mathbb{F}_q$ sú obe hodnoty u aj $u + a$ súčasne nenulové štvorce vidíme, že z predchádzajúcej vety je táto pravdepodobnosť takmer presne $1/4$. To môžeme interpretovať tak, že vlastnosť byť po pripočítaní hodnotou a štvorcom, je pravdepodobnostne nezávislá, až na zanedbateľnú chybu, na vlastnosti byť štvorcom. Vďaka tomu, že je 0 štvorcom, nie je táto pravdepodobnosť presne $1/4$.

Je prirodzené sa pýtať, ako vyzerá pravdepodobnosť, ak sú štvorcom nie 2 výrazy závislé na u, ale viacero výrazov. Ako naznačuje nasledujúca Veta 1.6, ktorá je pre túto prácu zásadná, i pri viacerých výrazoch platí niečo podobné, avšak odchýlka od ideálnej pravdepodobnosti rastie s počtom výrazov aj s ich polynómiálnou zložitosťou. Táto veta pracuje so zoznamom polynómov, ktoré splňujú určitú vlastnosť, ktorú nazveme bezštvorcovosť.

Definícia 1.5. *Majme $p_1, \ldots, p_k \in \mathbb{F}_q[x]$ zoznam polynómov. Povieme, že tento zoznam je **bezštvorcový**, ak žiaden podzoznam $p_{i_1}, \ldots, p_{i_r}$ tohto zoznamu, kde $1 \leq i_1 < \cdots < i_r \leq k$ a $r \geq 1$, nesplňuje, že $p_{i_1} \cdots p_{i_r}$ je štvorec (ako polynóm v algebraickom uzávere $\bar{\mathbb{F}}_q$ telesa $\mathbb{F}_q$).*

Veta 1.6. *Majme $p_1, \ldots, p_k \in \mathbb{F}_q[x]$ bezštvorcový zoznam polynómov stupňa $d_i \geq 1$, kde $i \in \{1, \ldots, k\}$, a $\varepsilon_1, \ldots, \varepsilon_k \in \{-1, 1\}$. Označme N počet všetkých $\alpha \in \mathbb{F}_q$, ktoré pre každé $i \in \{1, \ldots, k\}$ splňujú $\chi(p_i(\alpha)) = \varepsilon_i$. Potom*

$$\left| N - 2^{-k} q \right| < (\sqrt{q} + 1) D/2 - \sqrt{q}(1 - 2^{-k}) < (\sqrt{q} + 1) D/2, \tag{1.1}$$

kde $D = \sum_i d_i$.

Dôkaz. Dôkaz vety sa dá nájsť v [3, Theorem 1.4].

□

Skutočnosť, že nám Veta 1.6 vôbec umožňuje realizovať takéto asymptotické odhady, sa opiera o tvrdenie dokázané metódami algebraickej geometrie známe ako Weilov odhad. Uveďme pre úplnosť výkladu znenie tohto tvrdenia, ako je uvedené v [6, str. 162, Theorem 6.2.2].

Veta 1.7 (Weilov odhad). *Nech $f \in \mathbb{F}_q[x]$ je polynóm stupňa $d > 0$ a $\chi : \mathbb{F}_q^* \to \mathbb{C}^*$ je netriviálny multiplikatívny charakter rádu m (rozšírený o 0 na $\mathbb{F}_q$). Potom, ak f nie je m-tou mocninou polynómu v $\bar{\mathbb{F}}_q[x]$, kde $\bar{\mathbb{F}}_q$ je algebraický uzáver $\mathbb{F}_q$, potom platí*

$$\left| \sum_{x \in \mathbb{F}_q} \chi(f(x)) \right| \leq (d-1)\sqrt{q}.$$

Ako ďalší príklad použitia tohto odhadu môžeme spomenúť [7, Kapitola 3], kde je táto aplikácia podrobnejšie vysvetlená. Ako sa uvádza v [6], je tento odhad dôsledkom práce Weila v [8], kde je možné o tejto téme zistiť viac. Keďže sa však jedná o rozsiahle poznatky algebraickej geometrie, nebudeme sa tomuto odhadu podrobnejšie venovať a čitateľa odkážeme na uvedené zdroje.

Môžeme sa však pozrieť na Weilov odhad v kontexte Vety 1.4. Všimnime si, že ide istým spôsobom o jej zobecnenie a to tak, že každá pridaná polynomiálna podmienka znižuje počet α, ktoré vyhovujú požadovanej skupine podmienok zhruba o polovicu. Vďaka tomu je vidieť, že podmienky vo Vete 1.6 vyžadujúce, aby bola hodnota polynómu štvorec alebo neštvorec, sú na sebe asymptoticky nezávislé. To všetko však za splnenia predpokladu bezštvorcovosti uvedeného zoznamu polynómov. Dodajme, že pod asymptotickou nezávislosťou týchto podmienok myslíme to, že relatívna chyba sa limitne blíži nule. Weilov odhad nám však udáva, že je táto chyba tým väčšia, čím je väčší súčet stupňov polynómov.

1.2 Kvázigrupa

V tejto časti uvedieme definíciu kvázigrupy a tiež konštrukciu kvázigrupy pomocou kvadratického ortomorfizmu, čo je konštrukcia s ktorou budeme pracovať.

Definícia 1.8. ***Kvázigrupa*** $(Q, \cdot)$ *je množina Q s binárnou operáciou $\cdot$, ktorá spĺňuje, že pre každé $a, c \in Q$ existuje práve jedno $x \in Q$, ktoré spĺňuje $x \cdot a = c$ a zároveň pre každé $b, c \in Q$ existuje práve jedno $y \in Q$, ktoré spĺňuje $b \cdot y = c$.*

Všetky kvázigrupy, ktoré budeme v tomto texte uvažovať, budú konečné. Všimnime si tiež, že existuje vzťah medzi kvázigrupami rádu n a latinskými štvorcami rádu n a to taký, že latinský štvorec predstavuje tabuľku násobenia v kvázigrupe príslušného rádu. U kvázigrup nás bude zaujímať jedna špecifická vlastnosť - maximálna neasociativita.

Definícia 1.9. *Kvázigrupu $(Q, \cdot)$, ktorá spĺňuje*

$$\forall\, x, y, z \in Q: \quad x \cdot (y \cdot z) = (x \cdot y) \cdot z \quad \Longleftrightarrow \quad x = y = z \tag{1.2}$$

budeme označovať ***maximálne neasociatívna****.*

V článku [3] bolo dokázané, že maximálne neasociatívna kvázigrupa rádu q existuje pre každé $q \geq 9$ s určitými výnimkami, ktorými sú $q \in \{11, 12, 15, 40, 42, 44, 56, 66, 77, 88, 90, 110\}$ a tiež $q = 2p_1$ a $q = 2p_1p_2$, kde p_1, p_2 sú nepárne prvočísla spĺňujúce $p_1 \leq p_2 < 2p_1$. U týchto výnimiek však článok [3] nedokázal, že maximálne neasociatívna kvázigrupa príslušného rádu neexistuje, ale zatiaľ nebola nájdená konštrukcia maximálne neasociatívnej kvázigrupy daného rádu.

Ako sme už spomenuli v úvode, na článok [3] nadviazal článok [4], ktorý sa zaoberal asymptotickou hustotou maximálne neasociatívnych kvázigrup špeciálnej konštrukcie. Aby sme na to mohli nadviazať, musíme uviesť danú konštrukciu kvázigrupy, ktorá je založená na jednej z významných konštrukcií binárnej operácie kvázigrupy a to pomocou ortomorfizmu (z anglického orthomorphism) grupy.

Definícia 1.10. *Majme komutatívnu grupu $(G,+)$. Zobrazenie $\psi : G \to G$ budeme nazývať* ***ortomorfizmus*** *grupy G, ak je ψ permutácia a tiež zobrazenie $x \mapsto \psi(x) - x$ je permutácia. Ak navyše platí $\psi(0) = 0$, potom tento ortomorfizmus označujeme ako* ***kanonický****.*

Poznamenajme, že síce sme ortomorfizmus definovali iba pre komutatívnu grupu, je možné tento pojem zobecniť aj na nekomutatívne grupy.

Na základe každého ortomorfizmu grupy môžeme definovať binárnu operáciu kvázigrupy.

Lemma 1.11. *Majme ortomorfizmus ψ grupy $(G,+)$. Pre $\forall\, u, v \in G$ definujme binárnu operáciu $*$ na G vzťahom*

$$u * v = u + \psi(v - u). \tag{1.3}$$

Potom $(G,*)$ je kvázigrupa.

Dôkaz. Stačí overiť, že pre $v, w \in G$ existuje práve jedno $x \in G$ tak, že $x * v = w$ a pre $u, w \in G$ existuje práve jedno $y \in G$ tak, že $u * y = w$. Stačí si všimnúť, že ak $x * v = x + \psi(v - x) = w$, tak potom platí $\psi(v - x) - (v - x) = w - v$. Keďže z definície ψ je zobrazenie $x \mapsto \psi(x) - x$ permutácia, je zrejmé, že $v - x$ je určené jednoznačne a teda aj x je určené jednoznačne. V prípade $u * y = u + \psi(y - u) = w$ si stačí uvedomiť, že je ψ permutácia a teda $y - u$ je určené jednoznačne, z čoho dostávame, že aj y je určené jednoznačne. Z toho už je vidieť, že sa jedná o operáciu kvázigrupy.

□

V celom texte bude G aditivná grupa $\mathbb{F}_q$ rádu q, kde q je mocninou nepárneho prvočísla.

Veta 1.12. *Pre $a, b \in \mathbb{F}_q$ definujme zobrazenie $\psi = \psi_{a,b}$ tak, že pre $\forall\, u \in \mathbb{F}_q$ platí*

$$\psi(u) = \begin{cases} au & \text{ak je } u \text{ štvorec,} \\ bu & \text{ak nie je } u \text{ štvorec.} \end{cases} \tag{1.4}$$

Potom ψ je ortomorfizmus práve vtedy, keď ab aj $(1-a)(1-b)$ sú nenulové štvorce a zároveň $\{a, b\} \cap \{0, 1\} = \emptyset$.

Dôkaz. Dôkaz je uvedený v [9, Theorem 9.24, str.274].

□

Definícia 1.13. *Ortomorfizmus ψ spĺňujúci uvedené podmienky vo Vete 1.12 budeme nazývať* ***kvadratický ortomorfizmus****.*

Spojením (1.3) a (1.4) môžeme pre $a, b \in \mathbb{F}_q$ definovať binárnu operáciu $* = *_{a,b}$ na $\mathbb{F}_q$ tak, že $\forall\, u, v \in \mathbb{F}_q$ platí

$$u * v = \begin{cases} u + a(v-u) & \text{ak je } v-u \text{ štvorec,} \\ u + b(v-u) & \text{ak nie je } v-u \text{ štvorec.} \end{cases} \tag{1.5}$$

Táto operácia spĺňa vlastnosti binárnej operácie kvázigrupy práve vtedy, keď sú splnené predpoklady Vety 1.12 a teda zobrazenie ψ definované ako v (1.4) je ortomorfizmus.

Označenie 1.14. *Označne symbolom $\Sigma = \Sigma(\mathbb{F}_q)$ množinu všetkých $(a, b) \in \mathbb{F}_q \times \mathbb{F}_q$, ktoré splňujú predpoklady Vety 1.12 a teda: $\chi(ab) = 1$, $\chi((1-a)(1-b)) = 1$, $\{a, b\} \cap \{0{,}1\} = \emptyset$ a $a \neq b$.*

V definícií množiny Σ sme pridali dodatočnú podmienku $a \neq b$ a to z toho dôvodu, že v prípade $a = b$ je každá trojica $(v, u, v) \in \mathbb{F}_q^3$ asociatívna a teda kvázigrupa $(\mathbb{F}_q, *)$ nie je maximálne neasociatívna, čo pre nás nie je zaujímavé. Pripomeňme, že trojica (x, y, z) je asociatívna, keď platí $x \cdot (y \cdot z) = (x \cdot y) \cdot z$. Pre úplnosť výkladu sa pozrime na to, prečo to tak je. Predpokladajme teda, že $a = b$ a využime definíciu operácie $*$ ako v (1.5). Platí $(v * u) * v = (v + \psi(u - v)) * v = v + \psi(u - v) + \psi(-\psi(u - v)) = v + a(u - v) + a^2(v - u)$. Platí tiež $v*(u*v) = v*(u+\psi(v-u)) = v+\psi(u-v+\psi(v-u)) = v+a(u-v)+a^2(v-u)$. Z toho dostávame $(v * u) * v = v * (u * v)$.

Označenie 1.15. *Pre $(a, b) \in \Sigma$ označme kvázigrupu $(\mathbb{F}_q, *_{a,b})$ symbolom $Q_{a,b} = Q_{a,b}(\mathbb{F}_q)$, kde operácia $*_{a,b}$ je definovaná ako v* (1.5)

Ďalším krokom je definícia S a jej spojitosť s množinou Σ.

Označenie 1.16. *S je množina všetkých $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$ takých, že x aj y sú štvorce, $x \neq y$ a $\{x, y\} \cap \{0, 1\} = \emptyset$.*

V [4, Proposition 1.2] bolo dokázané, že existuje bijektívna transformácia medzi množinami Σ a S. Kedže je našim cieľom odhadnúť počet dvojíc $(a, b) \in \Sigma$, ktoré splňujú určité vlastnosti, môžeme na miesto toho odhadovať počet $(x, y) \in S$, na ktoré sa $(a, b) \in \Sigma$ zobrazia pomocou tejto bijektívnej transformácie. Tento postup volíme preto, lebo vlastnosti množiny S sa nám budú viac hodiť. Ešte uveďme ako vyzerá spomenutá bijektívna transformácia medzi Σ a S.

Veta 1.17. *[4, Proposition 1.2] Pre každé $(a, b) \in \Sigma$ existuje jedinečná dvojica $(x, y) \in S$, tak že platí*

$$a = \frac{x(1-y)}{x-y}, \quad b = \frac{1-y}{x-y}, \quad 1-a = \frac{y(1-x)}{y-x}, \quad a \quad 1-b = \frac{1-x}{y-x} \tag{1.6}$$

Zobrazenie

$$\Psi : \Sigma \to S, \quad (a, b) \mapsto \left(\frac{a}{b}, \frac{1-a}{1-b}\right) \tag{1.7}$$

je bijekcia. A ak $(x, y) \in S$, potom $\Psi^{-1}((x, y)) = (a, b)$ práve vtedy, keď platí (1.6).

Dôkaz. Dôkaz je uvedený v [4, Proposition 1.2].

□

Z toho priamo dostávame $|\Sigma(\mathbb{F}_q)| = |S(\mathbb{F}_q)|$. Navyše [4, Corollary 1.3] nám dáva, že $|S(\mathbb{F}_q)| = (q^2 - 8q + 15)/4$.

1.3 Rovnica asociativity

V ďalšej časti sa už zameráme na postup, ktorý využijeme pri asymptotických odhadoch počtu dvojíc $(x, y) \in S$ tak, aby pre $(a, b) = \Psi^{-1}((x, y))$ bola kvázigrupa $Q_{a,b}$ maximálne neasociatívna. Základná myšlienka ako zistiť, či je kvázigrupa $Q_{a,b}$ je maximálne neasociatívna, je pomocou rovnice asociativity.

Veta 1.18. *Kvázigrupa $Q_{a,b}$ je maximálne neasociatívna práve vtedy, keď jediným riešením rovnice*

$$\psi(\psi(u) - v) = \psi(-v) + \psi(u - v - \psi(-v)) \tag{1.8}$$

je $(u, v) = (0, 0)$. Ďalej platí, že dvojica $(u, v) \in \mathbb{F}_q \times \mathbb{F}_q$ je riešením rovnice (1.8) práve vtedy, keď $v * (0 * u) = (v * 0) * u$. Navyše, ak nejaká dvojica $(u, v) \neq (0, 0)$ spĺňuje (1.8), potom sú u, v, $\psi(u) - v$ a $u - v - \psi(-v)$ nenulové. Rovnicu (1.8) budeme nazývať ***rovnica asociativity****.*

Dôkaz. Dôkaz vety vychádza z [3, Lemma 1.3] v spojení s [3, Lemma 3.1].

Z Definície 1.9 maximálne neasociatívnej kvázigrupy musíme overiť, že platí

$$\forall\, x, y, z \in \mathbb{F}_q : \quad x * (y * z) = (x * y) * z \quad \Longleftrightarrow \quad x = y = z.$$

Využijeme vzťah (1.3). Platí

$$\begin{aligned} x * (y * z) =& x + \psi((y * z) - x) = x + \psi((y - x) + \psi(z - y)) \text{ a} \\ (x * y) * z =& (x + \psi(y - x)) * z = x + \psi(y - x) + \psi((z - x) - \psi(y - x)). \end{aligned}$$

Teda rovnosť $x * (y * z) = (x * y) * z$ nastáva práve vtedy, keď $\psi(\psi(u) - v) = \psi(-v) + \psi(u - v - \psi(-v))$, pre $v = x - y$ a $u = z - y$. Z toho je hneď vidieť, že $Q_{a,b}$ je maximálne neasociatívna práve vtedy, keď jediným riešením tejto rovnice je $(u, v) = (0, 0)$. Navyše, ak by bolo $u = 0$ a platila by rovnosť (1.8), potom tiež $v = 0$, pretože v takom prípady, by muselo platiť $0 = \psi(-v - \psi(-v))$. Naopak, ak by $v = 0$, potom tiež $u = 0$, pretože by v tomto prípade mala rovnica tvar $\psi^2(u) = \psi(u)$. Preto pri testovaní či dvojica (u, v) spĺňa rovnicu (1.8) stačí testovať dvojice bez nulových hodnôt.

Aby sme ukázali, že dvojica (u, v) je riešením rovnice (1.8) práve vtedy, keď $v * (0 * u) = (v * 0) * u$ stačí opäť použiť vzťah (1.3). Platí $0 * u = \psi(u)$ a $v * 0 = v + \psi(-v)$. Celkovo teda dostávame

$$\begin{aligned} v * (0 * u) =& v + \psi(\psi(u) - v) \text{ a} \\ (v * 0) * u =& v + \psi(-v) + \psi(u - v - \psi(-v)). \end{aligned}$$

Je vidno, že položením oboch výrazov do rovnice získame opäť rovnicu asociativity.

Ukázali sme, že dvojica (u, v) spĺňuje (1.8) práve vtedy, keď je trojica $(v, 0, u)$ asociatívna trojica v $Q_{a,b}$. Za predpokladu $(u, v) \neq (0, 0)$ a predpokladu, že je $(v, 0, u)$ asociatívna trojica platí, že $0 \notin \{u, v\}$, $v + \psi(-v) \neq u$ a tiež $v \neq \psi(u)$ vďaka čomu sú zrejme výrazy u, v, $\psi(u) - v$ a $u - v - \psi(-v)$ nenulové.

Ukážeme ešte, prečo platí $0 \notin \{u, v\}$, $v + \psi(-v) \neq u$ a $v \neq \psi(u)$ za predpokladov ako vyššie. Tu sa využije [3, Lemma 2.1], ktoré tvrdí, že pre idempotentnú

kvázigrupu Q a asociatívnu trojicu $(x, y, z) \in Q^3$ platí, že ak $x = y$ alebo $y = z$ alebo $x * y = z$ alebo $x = y * z$, potom $x = y = z$. Stačí si uvedomiť, že kvázigrupa $Q_{a,b}$ je idempotentná, teda že pre každé $u \in \mathbb{F}_q$ platí $u * u = u$, čo je vidno priamo z definície operácie $*$ uvedenej v (1.5). Vychádzame z predpokladu $(u, v) \neq (0, 0)$ z čoho tiež plynie, že $x \neq y$ a $y \neq z$. Aplikujeme [3, Lemma 2.1] na asociatívnu trojicu $(v, 0, u)$ ako sme ju uviedli vyššie a dostávame, že musí platiť $u \neq 0$, $v \neq 0$, $v * 0 \neq u$ a $v \neq 0 * u$. Z čoho plynie $0 \notin \{u, v\}$, $v + \psi(-v) \neq u$ a $v \neq \psi(u)$.

□

Z predchádzajúcej vety je vidieť, že v závislosti na hodnotách $\chi(u)$, $\chi(-v)$, $\chi(\psi(u) - v)$ a $\chi(u - v - \psi(-v))$ môže byť rovnica asociativity transformovaná na lineárnu rovnicu s neznámymi u a v. Pritom pre $a, b \in \Sigma$ využívame definíciu kvadratického ortomorfizmu ψ ako v (1.5). Každý výskyt ψ v rovnici asociativity (1.8) nahradíme podľa (1.5). Kedže výsledný tvar rovnice asociativity bude rôzny v závislosti na hodnotách $\chi(u)$, $\chi(-v)$, $\chi(\psi(u) - v)$ a $\chi(u - v - \psi(-v))$ zavedieme si pre $i, j, r, s \in \{0, 1\}$ nasledujúce označenie

$$\begin{aligned} i = 0 &\iff \chi(u) = 1, \\ j = 0 &\iff \chi(-v) = 1, \\ r = 0 &\iff \chi(\psi(u) - v) = 1 \text{ a} \\ s = 0 &\iff \chi(u - v - \psi(-v)) = 1. \end{aligned}$$

V prípade, že nejaký výraz u, $-v$, $\psi(u) - v$ alebo $u - v - \psi(-v)$ nie je štvorec, tak sa príslušná hodnota i, j, r alebo s zmení na 1. Prípad, že by nejaký z týchto 4 výrazov nadobúdal hodnotu 0 neuvažujeme, pretože vo Vete 1.18 sme ukázali, že ak nejaká nenulová dvojica splňuje rovnicu asociativity, tak sú všetky tieto výrazy tiež nenulové.

Je pekne vidieť, že štvoricu (i, j, r, s) môžeme zvoliť 16 rôznymi spôsobmi a preto aj rovnica asociativity môže mať 16 rôznych tvarov. To budeme v ďalšej časti využívať.

Označenie 1.19. *Pre $(a, b) \in \Sigma$ označme $E(a, b)$ množinu dvojíc $(u, v) \neq (0, 0)$, ktoré splňujú rovnicu asociativity (1.8). Pre dané (a, b) a štvoricu $(i, j, r, s) \in \{0, 1\}^4$ označme $E_{ij}^{rs}(a, b)$ množinu takých $(u, v) \in E(a, b)$, pre ktoré navyše platí $i = \chi(u)$, $j = \chi(-v)$, $r = \chi(\psi(u) - v)$ a $s = \chi(u - v - \psi(-v))$.*

Týmto spôsobom sme získali 16 disjunktných množín $E_{ij}^{rs}(a, b)$ takých, že $E(a, b) = \bigcup E_{ij}^{rs}(a, b)$. Priamo z definície množiny $E(a, b)$ v kombinácií s Vetou 1.18 dostávame nasledujúci dôsledok.

Dôsledok 1.20. *Kvázigrupa $Q_{a,b}$ je maximálne neasociatívna práve vtedy, keď $E(a, b) = \emptyset$.*

Z dôsledku plynie, že počet dvojíc $(a, b) \in \Sigma$, pre ktoré je $Q_{a,b}$ maximálne neasociatívna, môžeme spočítať nepriamo a to ako počet (a, b), pre ktoré $E(a, b) = \emptyset$.

Označenie 1.21. *Pre $i, j, r, s \in \{0, 1\}$ označíme*

$$\Sigma_{ij}^{rs} = \{(a, b) \in \Sigma : E_{ij}^{rs}(a, b) \neq \emptyset\}.$$

Priamo z definície množiny Σ_{ij}^{rs} plynie ďalší dôsledok a tým je ďalšia ekvivalencia k Vete 1.18 a k Dôsledku 1.20.

Dôsledok 1.22. *Kvázigrupa $Q_{a,b}$ je maximálne neasociatívna práve vtedy, keď $(a,b) \notin \bigcup \Sigma_{ij}^{rs}$.*

Definícia 1.23. *Pre $i,j,r,s \in \{0,1\}$ definujeme množinu S_{ij}^{rs} tak, že platí*

$$S_{ij}^{rs} = \{(x,y) \in S : \Psi^{-1}((x,y)) \in \Sigma_{ij}^{rs}\},$$

kde Ψ je bijekcia definovaná vzťahom (1.7).

Predchádzajúcu definíciu by sme kompaktne mohli zapísať ako

$$S_{ij}^{rs} = \Psi(\Sigma_{ij}^{rs}).$$

Práve množiny S_{ij}^{rs} budú hrať kľúčovú úlohu vo zvyšku našej práce. Spojením Dôsledku 1.22 s definíciou množín S_{ij}^{rs} dostávame nasledujúci kľúčový dôsledok.

Dôsledok 1.24. *Počet dvojíc $(a,b) \in \Sigma$ takých, že $Q_{a,b}$ je maximálne neasociatívna kvázigrupa je rovný veľkosti množiny $S \setminus \bigcup S_{ij}^{rs}$.*

Predchádzajúci dôsledok bude pre nás veľmi dôležitý a využijeme ho pri odhadoch počtu dvojíc (a,b), pre ktoré je $Q_{a,b}$ maximálne neasociatívna kvázigrupa. Asymptotický odhad sa bude na základe tohto dôsledku počítať tak, že určíme asymptotickú veľkosť $S \setminus \bigcup S_{ij}^{rs}$. Z toho dôvodu budeme potrebovať spôsob na popísanie množín S_{ij}^{rs}, ktorý nám umožní získať potrebný odhad.

V článku [4] je venovaná celá 2. kapitola popisu množín S_{ij}^{rs} na základe toho, že hodnoty určitých polynómov v x a y sú po dosadení $(x,y) \in S$ buď štvorce alebo nie sú štvorce. Základná myšlienka postupu, ako sa k takému popisu množín S_{ij}^{rs} dospeje, je založená na rôznych tvaroch rovnice asociativity v závislosti na štvorici (i,j,r,s) a následnými úpravami s využitím bijekcie Ψ sa dospeje k hľadaným polynómom pre každú množinu S_{ij}^{rs}.

Pri hľadaní polynómov, ktoré určujú pre ktorú štvoricu (i,j,r,s) platí $(x,y) \in S_{ij}^{rs}$, budeme nezávisle na sebe skúmať 2 prípady v závislosti na q. V prvom prípade predpokladáme $q \equiv 1 \bmod 4$, čo znamená, že $\chi(-1) = 1$. V druhom prípade zas $q \equiv 3 \bmod 4$, čo je ekvivalentné tomu, že platí $\chi(-1) = -1$. Pri tomto rozlíšení na 2 situácie sa navyše v predchádzajúcom článku ukázalo, že sú niektoré množiny S_{ij}^{rs} prázdne.

Pre prípad $q \equiv 1 \bmod 4$ obsahuje [4, Theorem 2.10] podrobný zoznam tých množín S_{ij}^{rs}, ktoré sú v tomto prípade prázdne, a pre neprázdne množiny obsahuje podmienky, ktoré musí spĺňovať dvojica (x,y), aby patrila do danej množiny S_{ij}^{rs}. Pre prípad $q \equiv 3 \bmod 4$ je to isté uvedené v [4, Theorem 2.11]. Ako sme už uviedli, tieto podmienky vychádzajú z rôznych tvarov rovnice asociativity v závislosti na štvorici (i,j,r,s) a ich odvodenie je pomerne pracné a nebudeme ho v tejto práci uvádzať.

Obe tvrdenia za malú chvíľu uvedieme, ale ešte pred tým si zavedieme označenie určitých polynómov, ktoré budeme pre prehľadnosť zápisu v ďalšej časti používať.

Označenie 1.25. *Vo zvyšku textu budeme pracovať s určitými polynómami v x a y, ktoré budeme pre prehľadnosť označovať nasledujúcim spôsobom*

$$\begin{aligned} f_1(x,y) &= x^2+y^2-xy-x, & f_2(x,y) &= x^2+y^2-xy-y,\\ f_3(x,y) &= y^2x+xy-x^2-y^2, & f_4(x,y) &= x^2y+xy-x^2-y^2,\\ g_1(x,y) &= x^2+y-2x, & g_2(x,y) &= y^2+x-2y,\\ g_3(x,y) &= x^2+y-2xy, \quad a & g_4(x,y) &= y^2+x-2xy. \end{aligned}$$

Tvrdenie 1.26. *[4, Theorem 2.10.] Predpokladajme, že $q \equiv 1 \bmod 4$ je mocnina prvočísla a množina S je ako v Označení 1.16. Nech $(x,y) \in S$ spĺňajú*

$$\begin{aligned} &[y+1-x \neq 0 \text{ alebo } x^2-x-1 \neq 0] \text{ a zároveň}\\ &[x+1-y \neq 0 \text{ alebo } y^2-y-1 \neq 0]. \end{aligned} \tag{1.9}$$

Potom množiny S_{01}^{00}, S_{01}^{10}, S_{01}^{11}, S_{10}^{00}, S_{10}^{01} a S_{10}^{11} sú prázdne a $S_{11}^{11} = S_{00}^{00}$. Položme $\varepsilon = \chi(x-y)$. Potom

$$\begin{aligned}
&(x,y) \in S_{00}^{00} \iff \chi(1-x) = \chi(1-y) = \varepsilon,\\
&(x,y) \in S_{11}^{00} \iff \chi(f_1(x,y)) = \chi(f_2(x,y)) = -\varepsilon,\\
&(x,y) \in S_{00}^{11} \iff \chi(f_3(x,y)) = \chi(f_4(x,y)) = -\varepsilon,\\
&(x,y) \in S_{11}^{01} \iff \chi(1-x) = -\varepsilon, \chi(y+1-x) = 1 \text{ a } \chi(f_1(x,y)) = \varepsilon,\\
&(x,y) \in S_{11}^{10} \iff \chi(1-y) = -\varepsilon, \chi(x+1-y) = 1 \text{ a } \chi(f_2(x,y)) = \varepsilon,\\
&(x,y) \in S_{00}^{10} \iff \chi(1-x) = -\varepsilon, \chi(x+xy-y) = 1 \text{ a } \chi(f_3(x,y)) = \varepsilon,\\
&(x,y) \in S_{00}^{01} \iff \chi(1-y) = -\varepsilon, \chi(y+xy-x) = 1 \text{ a } \chi(f_4(x,y)) = \varepsilon,\\
&(x,y) \in S_{01}^{01} \iff \chi(y+xy-x) = -\eta, \chi(g_1(x,y)) = -\eta\varepsilon \text{ a } \chi(g_4(x,y)) = \eta\varepsilon,\\
&\qquad\qquad \text{kde } \eta = \chi(y+1-x),\\
&(x,y) \in S_{10}^{10} \iff \chi(x+xy-y) = -\eta, \chi(g_2(x,y)) = -\eta\varepsilon \text{ a } \chi(g_3(x,y)) = \eta\varepsilon,\\
&\qquad\qquad \text{kde } \eta = \chi(x+1-y).
\end{aligned}$$

Dôkaz. Dôkaz tvrdenia je rozdelený do viacerých technických lemmat v [4, Kapitola 2].

□

Tvrdenie 1.27. *[4, Theorem 2.11.] Predpokladajme, že $q \equiv 3 \bmod 4$ je mocnina prvočísla a množina S je ako v Označení 1.16. Nech $(x,y) \in S$ spĺňajú*

$$\begin{aligned} &[y+1-x \neq 0 \text{ alebo } x^2-x-1 \neq 0] \text{ a zároveň}\\ &[x+1-y \neq 0 \text{ alebo } y^2-y-1 \neq 0]. \end{aligned} \tag{1.10}$$

Potom množiny S_{00}^{00}, S_{00}^{11}, S_{11}^{00}, S_{11}^{11} *sú prázdne,* $S_{10}^{01} = S_{01}^{10}$ *a platí*

$$\begin{aligned}
(x,y) \in S_{01}^{10} &\iff \chi((1-y)(x-y)) = \chi((1-x)(y-x)) = 1,\\
(x,y) \in S_{01}^{00} &\iff \chi((1-x)(x-y)) = \chi(g_1(x,y)(y-x)) = 1,\\
(x,y) \in S_{10}^{00} &\iff \chi((1-y)(y-x)) = \chi(g_2(x,y)(x-y)) = 1,\\
(x,y) \in S_{10}^{11} &\iff \chi((1-x)(x-y)) = \chi(g_3(x,y)(x-y)) = 1,\\
(x,y) \in S_{01}^{11} &\iff \chi((1-y)(y-x)) = \chi(g_4(x,y)(y-x)) = 1,\\
(x,y) \in S_{11}^{01} &\iff \chi((1-x)(x-y)) = \chi(x-1-y) = \chi((x-y)f_1(x,y)) = 1,\\
(x,y) \in S_{11}^{10} &\iff \chi((1-y)(y-x)) = \chi(y-1-x) = \chi((y-x)f_2(x,y)) = 1,\\
(x,y) \in S_{00}^{10} &\iff \chi((1-x)(x-y)) = \chi(y-xy-x) = \chi((x-y)f_3(x,y)) = 1,\\
(x,y) \in S_{00}^{01} &\iff \chi((1-y)(y-x)) = \chi(x-xy-y) = \chi((y-x)f_4(x,y)) = 1,\\
(x,y) \in S_{01}^{01} &\iff \chi((x-xy-y)(x-1-y)) = \chi(g_1(x,y)(y-x)(x-1-y)) =\\
&\qquad = \chi(g_4(x,y)(y-x)(x-1-y)) = 1,\\
(x,y) \in S_{10}^{10} &\iff \chi((y-xy-x)(y-1-x)) = \chi(g_2(x,y)(x-y)(y-1-x)) =\\
&\qquad = \chi(g_3(x,y)(x-y)(y-1-x)) = 1.
\end{aligned}$$

Dôkaz. Dôkaz tvrdenia je rozdelený do viacerých technických lemmat v [4, Kapitola 2].

□

V Tvrdeniach 1.26 a 1.27 ako aj v ďalšej časti je veľmi dôležitý kvadratický charakter, preto pre pripomenutie odkážeme čitateľa na jeho Definíciu 1.2.

Dodajme ešte, že vzťahy (1.9) a (1.10) z predpokladov predchádzajúcich tvrdení môžu byť za určitých okolností v tejto práci porušené. To však nebude mať vplyv na asymptotické odhady, ktoré budeme počítať. Vysvetlenie tejto skutočnosti je uvedené v sekcii 1.5.

Sústreďme sa na neprázdne množiny z vyššie uvedených tvrdení. U každej z nich je uvedená nejaká skupina podmienok. Každá z týchto podmienok je daná hodnotou kvadratického charakteru nejakého polynómu v x a y. Teda pre nejaké $\omega \in \{1,-1\}$ a polynóm $p(x,y) \in \mathbb{F}_q[x,y]$ nám konkrétna podmienka dáva množinu $\{(x,y) \in S : \chi(p(x,y)) = \omega\}$. Pre lepšiu orientáciu v ďalšej časti práci si zaveďme zjednodušené označenie tejto množiny.

Označenie 1.28. *Majme polynóm* $p(x,y) \in \mathbb{F}_q[x,y]$ *a* $\omega \in \{1,-1,0\}$. *Pre množinu danú hodnotou kvadratického charakteru polynómu* $p(x,y)$ *budeme používať označenie*

$$\langle p(x,y), \omega \rangle = \{(x,y) \in S : \chi(p(x,y)) = \omega\}.$$

Na základe tohto označenia je jednoduché si uvedomiť, že pre každú štvoricu $(i,j,r,s) \in \{0,1\}^4$ môžeme vyjadriť množinu S_{ij}^{rs} pomocou vhodných polynómov $p_1^{(i,j,r,s)}(x,y), \ldots, p_k^{(i,j,r,s)}(x,y) \in \mathbb{F}_q[x,y]$ a $\omega_1^{(i,j,r,s)}, \ldots, \omega_k^{(i,j,r,s)} \in \{1,-1\}$ ako

$$S_{ij}^{rs} = \bigcap_{1 \le e \le k} \langle p_e^{(i,j,r,s)}(x,y), \omega_e^{(i,j,r,s)} \rangle, \tag{1.11}$$

kde v závislosti na štvorici (i,j,r,s) je $k \in \{2,3\}$.

Použili sme označenie $p_e^{(i,j,r,s)}(x,y)$ a $\omega_e^{(i,j,r,s)}$ aby sme zdôraznili, že dané polynómy a príslušné hodnoty ω sú závislé na štvorici (i,j,r,s). V častiach práce, keď bude jasné s akou množinou S_{ij}^{rs} pracujeme, budeme jednoducho písať $p_e(x,y)$ a ω_e.

1.4 Obecný popis množiny T

Vráťme sa k Dôsledku 1.24 a pozrime sa na neho cez značenie definované na konci predchádzajúcej sekcie. Zaujíma nás asymptotický odhad veľkosti množiny $S \setminus \bigcup S_{ij}^{rs}$, ktorú označme T. Zrejme tiež platí $T = \bigcap \overline{S_{ij}^{rs}}$, kde $\overline{S_{ij}^{rs}} = S \setminus S_{ij}^{rs}$. Využime vyjadrenie množiny S_{ij}^{rs} uvedené v (1.11) a vyjadrime pomocou neho množinu $\overline{S_{ij}^{rs}}$. Zrejme platí

$$\overline{S_{ij}^{rs}} = \bigcup_{1 \le e \le k} \overline{\langle p_e^{(i,j,r,s)}(x,y), \omega_e^{(i,j,r,s)} \rangle}, \tag{1.12}$$

kde $\overline{\langle p_e^{(i,j,r,s)}(x,y), \omega_e^{(i,j,r,s)} \rangle}$ označuje doplnok množiny $\langle p_e^{(i,j,r,s)}(x,y), \omega_e^{(i,j,r,s)} \rangle$ v S.

Ako vyzerá doplnok $\langle p(x,y), \omega \rangle$ v S? Je vidieť, že

$$\overline{\langle p(x,y), \omega \rangle} = \langle p(x,y), -\omega \rangle \cup \langle p(x,y), 0 \rangle.$$

Keďže platí $T = \bigcap \overline{S_{ij}^{rs}}$, tak množinu T môžeme rozdeliť na 2 množiny T^* a T_0 tak, že $T = T^* \bigcup T_0$, kde

$$T^* = \bigcap_{(i,j,r,s) \in \{0,1\}^4} \left(\bigcup_{1 \le e \le k} \langle p_e^{(i,j,r,s)}(x,y), -\omega_e^{(i,j,r,s)} \rangle \right) \text{ a} \tag{1.13}$$

$$T_0 = \bigcap_{(i,j,r,s) \in \{0,1\}^4} \left(\bigcup_{1 \le e \le k} \langle p_e^{(i,j,r,s)}(x,y), 0 \rangle \right)$$

kde v závislosti na štvorici (i,j,r,s) je $k \in \{2,3\}$.

Prípadov, kedy je (x,y) koreňom nejakého z polynómov použitých pri popise množiny T je málo a pri asymptotickom odhade ich môžeme zanedbať, čo v zmysle zavedeného označenia znamená zanedbanie množiny T_0. Preto pre asymptotický odhad veľkosti množiny T využijeme iba popis množiny T^* ako sme ho uviedli vo vzťahu (1.13).

Vo všetkých prípadoch, ktoré budeme v tejto práci rozoberať budeme vychádzať z popisu množiny T^* uvedeného v (1.13) a s jeho využitím budeme odhadovať asymptotickú veľkosť množiny T pomocou Vety 1.6. Ako sme uviedli v predchádzajcej sekcii množinu T_0 zanedbáme, preto je asymptotický odhad veľkosti množiny T zároveň asymptotickým odhadom veľkosti množiny T^*.

Využijeme teda popis množiny T^* odvodený z množín S_{ij}^{rs} a využijeme skutočnosť, že tieto množiny sú dané hodnotou kvadratického charakteru určitých polynómov presne tak, ako je to v Tvrdení 1.26 a v Tvrdení 1.27. Obecný postup bude teda taký, že vhodným spôsobom určíme zoznam polynómov, ktoré sa využijú pri popise T^* podľa vzťahu (1.13) a na zoznam týchto polynómov aplikujeme Vetu 1.6, čím získame hľadaný asymptotický odhad.

1.5 Cieľ práce - špeciálne situácie

Máme pripravené všetky potrebné konštrukcie, aby sme sa mohli pustiť do samotných výpočtov, ktoré sú hlavným prínosom tejto práce. Na záver prvej kapitoly nám už ostáva uviesť iba polynómy, ktoré určujú dodatočný vzťah medzi x a y v množine S, pre ktoré budeme vo zvyšku práce hľadať asymptotický odhad veľkosti množiny T. Ide o polynómy uvedené na záver článku [4, Kapitola 6 - Conclusions]. Tie polynómy sú:

- $t_1(x, y) = x - 1 - y$,
- $t_2(x, y) = x - xy - y$,
- $t_3(x, y) = y - 1 - x$,
- $t_4(x, y) = y - xy - x$,
- $t_{4+j}(x, y) = f_j(x, y)$, pre $j \in \{1, 2, 3, 4\}$ a
- $t_{8+j}(x, y) = g_j(x, y)$, pre $j \in \{1, 2, 3, 4\}$.

Opäť využívame označenie polynómov $f_j(x, y)$ a $g_j(x, y)$ ako sme ich definovali v Označení 1.25.

Dodatočný vzťah medzi x a y bude daný tým, že pre nejaké $i \in \{1, \ldots, 12\}$ budeme predpokladať $t_i(x, y) = 0$.

Veta 1.29. *Zobrazenia $(x, y) \mapsto (y, x)$ a $(x, y) \mapsto (x^{-1}, y^{-1})$ permututujú množinu S.*

Dôkaz. Priamo z definície množiny S platí, že $(x, y) \in S$ práve vtedy, keď x aj y sú rôzne štvorce a navyše $\{x, y\} \cap \{0, 1\} = \emptyset$. Obe zobrazenia v znení vety zachovávajú tieto vlastnosti, pretože (y, x) aj (x^{-1}, y^{-1}) sú za predpokladu $(x, y) \in S$ opäť dvojice, ktoré splňujú všetky podmienky na náležanie do množiny S. Preto ide skutočne o permutácie množiny S.

□

Práve uvedené permutácie majú ešte jednu peknú vlastnosť, ktorú pre úplnosť uvedieme.

Dôsledok 1.30. *[4, Proposition 2.3.] Pre $i, j, r, s \in \{0, 1\}$ platí*

$$(x, y) \in S_{ij}^{rs} \iff (y, x) \in S_{ji}^{sr} \iff (x^{-1}, y^{-1}) \in S_{1-i,1-j}^{1-r,1-s}.$$

Dôkaz. Dôkaz je uvedený v [4, Proposition 2.3.].

□

Pozrime sa na vyššie uvedených 12 speciálnych prípadov, ktoré sme si dali za úlohu preskúmať, a určíme na aké prípady sa dajú aplikovať permutácie uvedené vo Vete 1.29, ktorých využitím by sme v konečnom dôsledku vystačili s preskúmaním nižšieho počtu špeciálnych prípadov. Prípady, ktoré sa na seba dajú pomocou uvedených permutácií previesť, by mali rovnaké asymptotické vlastnosti. V prípade zobrazenia $(x, y) \mapsto (y, x)$ je to zrejmé. U zobrazenia $(x, y) \mapsto (x^{-1}, y^{-1})$ sa využíva vlastnosť reciprokého polynómu.

Definícia 1.31. *Pre polynóm $p(x,y) \in \mathbb{F}_q[x,y]$ tak, že $x \nmid p(x,y)$ a $y \nmid p(x,y)$, definujeme reciproký polynóm $\widehat{p}(x,y)$ ako polynóm $x^n y^m p(x^{-1}, y^{-1})$, kde n a m sú najvyššie mocniny x a y v polynóme $p(x,y)$.*

Keďže $(x,y) \in S$, a teda x a y sú štvorce, platí pre nejaký polynóm $p(x,y) \in \mathbb{F}_q[x,y]$ nasledujúce:

$$\chi(\hat{p}(x,y)) = \chi(x^n y^m p(x^{-1}, y^{-1})) = \chi(p(x^{-1}, y^{-1})). \tag{1.14}$$

Využitím práve uvedených vlastností si môžeme všimnúť, že platí

- $t_1(x,y) = \widehat{t_2}(y,x) = t_3(y,x) = \widehat{t_4}(x,y)$,
- $f_1(x,y) = f_2(y,x) = -\widehat{f_3}(x,y) = -\widehat{f_4}(y,x)$ a
- $g_1(x,y) = g_2(y,x) = \widehat{g_3}(x,y) = \widehat{g_4}(y,x)$.

Vďaka tejto skutočnosti si vystačíme s asymptotickým odhadom v 3 situáciách a to sú prípady, keď je dodatočný vzťah medzi x a y daný jedným z polynómov $t_1(x,y)$, $f_1(x,y)$ alebo $g_1(x,y)$. Práve týmto prípadom sa vo zvyšku práce budeme venovať.

Otázkou zostáva, prečo sú práve polynómy $t_i(x,y)$ zaujímavé. V článku [4] sa počítal asymptotický odhad veľkosti množiny T, z ktorej bolo nutné odstrániť tie dvojice (x,y), pre ktoré platilo $t_i(x,y) = 0$, pre nejaké $i \in \{1, \ldots, 12\}$. Tento požiadavok vznikol tak, že sa po dosadení ľubovoľnej konštanty $c \in \mathbb{F}_q$ na pozíciu druhej premennej v zozname polynómov vstupujúcom do asymptotických odhadov požadovalo, aby výsledkom po dosadení bol bezštvorcový zoznam polynómov v jednej premennej. Skúmaniu podmienok, ktoré museli byť splnené, aby bol tento zoznam polynómov v jednej premennej bezštvorcový sa venuje [4, Kapitola 3 - Avoiding squares]. Keďže sa $(x,y) \in S$, ktoré pre nejaké i spĺňovali $t_i(x,y) = 0$ vôbec neúčasnili odhadu veľkosti T, je na mieste skúmať asymptotické chovanie na nulových bodoch každého z týchto polynómov, pretože nás táto situácia vedie k predpokladu, že by toto asymptotické chovanie mohlo byť výrazne odlišné od výsledkov článku [4].

Uveďme ešte ako využijeme asymptotický odhad veľkosti množiny T. Rovnako ako v článku [4] je naším cieľom určenie pravdepodobnosti, že pri náhodnej voľbe $(a,b) \in \Sigma$ bude kvázigrupa $Q_{a,b}$ maximálne neasociatívna. V článku [4] sa najprv určila asymptotická veľkosť množiny T, ktorá sa porovnala s veľkosťou množiny S, respektíve Σ. Výsledkom toho bola pravdepodobnosť, že náhodne zvolená dvojica $(x,y) \in S$ padne do T, čo je ekvivalentné tomu, že pre $(a,b) = \Psi^{-1}((x,y))$ je $Q_{a,b}$ maximálne neasociatívna (využívame bijekciu Ψ definovanú vzťahom (1.7)). V našej práci budeme postupovať rovnako až na to, že dvojice (x,y) nebudeme brať z celého S, ale z nejakého S'. Množina S' sa bude pre jednotlivé skúmané prípady líšiť, bude však vždy obsahovať iba tie dvojice $(x,y) \in S$, ktoré budú v danom prípade spĺňať dodatočnú podmienku $t_i(x,y) = 0$. Takže pravdepodobnosť, ktorú budeme hľadať, bude pravdepodobnosť, že náhodne zvolené $(x,y) \in S'$ padne do T.

V predpokladoch (1.9) Tvrdenia 1.26 a v predpokladoch (1.10) Tvrdenia 1.27 sa pre $(x,y) \in S$ vyžaduje

$$[y + 1 - x \neq 0 \text{ alebo } x^2 - x - 1 \neq 0] \text{ a zároveň}$$
$$[x + 1 - y \neq 0 \text{ alebo } y^2 - y - 1 \neq 0].$$

Je zrejmé, že podmienky $y+1-x \neq 0$ a $x+1-y \neq 0$ kolidujú s dvoma prípadmi, ktoré sme si dali za úlohu preskúmať a to $t_1(x,y) = 0$ a $t_3(x,y) = 0$. Podľa [4, Remark 2.9] sú však najviac 2 dvojice $(x,y) \in S$, ktoré spĺňujú $y + 1 - x = 0$ a zároveň $x^2 - x - 1 = 0$ a rovnako maximálne 2 dvojice, ktoré spĺňujú $x+1-y = 0$ a $y^2 - y - 1 = 0$ a teda predpoklady (1.9) a (1.10) by v prípade $t_1(x,y) = 0$ alebo $t_3(x,y) = 0$ neboli zásadne porušené, pretože tých prípadov je len veľmi málo a pri asymptotických odhadoch ich môžeme zanedbať.

2. $t_1(x, y) = 0$

Výpočtovú časť práce teda začneme tým, že Tvrdenie 1.26 a tiež Tvrdenie 1.27 uvedieme v podobe, ktorá využíva dodatočný predpoklad $t_1(x, y) = 0$ a tieto tvrdenia následne využijeme k asymptotickým odhadom veľkosti množiny T^*. Rovnaký postup bude použitý aj pre prípady využívajúce predpoklad $f_1(x, y) = 0$ a $g_1(x, y) = 0$, ktoré budú uvedené v ďalších kapitolách.

2.1 Tvrdenie 1.26 pre prípad $t_1(x, y) = 0$

Základným kameňom pre popis množiny T^* je popis množín S_{ij}^{rs}. V tejto sekcii sa zameráme na Tvrdenie 1.26 a uvedieme podmienky pre množiny S_{ij}^{rs}, ktoré musí spĺňať $(x, y) \in S$, aby $(x, y) \in S_{ij}^{rs}$, a to všetko za dodatočnej podmienky, že je daný vzťah medzi x a y taký, že pre polynóm $t_1(x, y) = x - 1 - y$ platí $t_1(x, y) = 0$. Z čoho plynie, že $x = y + 1$. V takom prípade budú polynómy uvedené v podmienkach iba v jednej neznámej y a na miesto dvojice (x, y) budeme písať $(y + 1, y)$. Následne využijeme popisy množín S_{ij}^{rs} za uvedenej dodatočnej podmienky pre odhad veľkosti množiny T v sekciách 2.3.1 a 2.3.2.

Lemma 2.1. *Podmienky pre neprázdne množiny S_{ij}^{rs} uvedené v Tvrdení 1.26 majú v prípade dodatočnej podmienky $t_1(x, y) = 0$ tvar:*

- *V prípade $q \equiv 1 \bmod 8$ platí:*

$$
\begin{aligned}
S_{11}^{00} = S_{11}^{01} = S_{00}^{10} = & S_{01}^{01} = \emptyset \\
(y+1, y) \in S_{00}^{00} &\iff \chi(1-y) = 1 \\
(y+1, y) \in S_{00}^{11} &\iff \chi(y^3 - y - 1) = \chi(y^3 + y^2 - 1) = -1 \\
(y+1, y) \in S_{11}^{10} &\iff \chi(1-y) = -1 \ a \ \chi(y^2 + 1) = 1 \\
(y+1, y) \in S_{00}^{01} &\iff \chi(y^2 + y - 1) = \chi(y^3 + y^2 - 1) = 1 \ a \ \chi(1-y) = -1 \\
(y+1, y) \in S_{10}^{10} &\iff \chi(y^2 + y + 1) = \chi(y^2 - y + 1) = -1 \ a \\
&\qquad \chi(-y^2 + y + 1) = 1
\end{aligned}
$$

- *V prípade $q \equiv 5 \bmod 8$ platí:*

$$
\begin{aligned}
S_{11}^{00} = S_{11}^{01} = S_{00}^{10} = & S_{01}^{01} = S_{11}^{10} = \emptyset \\
(y+1, y) \in S_{00}^{00} &\iff \chi(1-y) = 1 \\
(y+1, y) \in S_{00}^{11} &\iff \chi(y^3 - y - 1) = \chi(y^3 + y^2 - 1) = -1 \\
(y+1, y) \in S_{00}^{01} &\iff \chi(y^2 + y - 1) = \chi(y^3 + y^2 - 1) = 1 \ a \ \chi(1-y) = -1 \\
(y+1, y) \in S_{10}^{10} &\iff \chi(y^2 + y + 1) = \chi(y^2 - y + 1) = 1 \ a \\
&\qquad \chi(-y^2 + y + 1) = -1
\end{aligned}
$$

Dôkaz. Keďže jedným z predpokladov Tvrdenia 1.26 je $q \equiv 1 \bmod 4$ (teda -1 je štvorec alebo tiež $\chi(-1) = 1$), budeme to v celom dôkaze predpokladať.

Tvrdenie 1.26 uvádza $\varepsilon = \chi(x-y)$. Využitím predpokladu $x = y+1$ dostávame $\varepsilon = \chi(x - y) \overset{x=y+1}{=} \chi(y + 1 - y) = \chi(1) = 1$.

Do pôvodnej podoby tohto tvrdenia teda dosadíme $x = y + 1$ a $\varepsilon = 1$ a určíme, ako vyzerajú jednotlivé podmienky pre množiny S_{ij}^{rs} využitím predpokladu $\chi(-1) = 1$ a ďalších vlastností kvadratického charakteru χ.

Množina S_{11}^{00} je prázdna, pretože podmienka $\chi(f_1(x, y)) \overset{x=y+1}{=} \chi(y^2) = -1$ nemá riešenie, keďže $\chi(y^2) = 1, \forall y \in \mathbb{F}_q$.

Množiny S_{11}^{01} a S_{00}^{10} sú prázdne, pretože v oboch prípadoch podmienka $\chi(1 - x) \overset{x=y+1}{=} \chi(-y) = -1$ nemá riešenie, keďže predpokladáme $\chi(-1) = 1$ a $\chi(y) = 1$.

V prípade S_{00}^{00} majú podmienky po dosadení za x a ε tvar

- $\chi(1 - x) \overset{x=y+1}{=} \chi(-y) = 1$ (platí vždy z predpokladu $\chi(-1) = 1$ a $\chi(y) = 1$ z definície S),
- $\chi(1 - y) = 1$.

V prípade S_{00}^{11} majú podmienky tvar

- $\chi(f_3(x, y)) \overset{x=y+1}{=} \chi(y^3 - y - 1) = -1$,
- $\chi(f_4(x, y)) \overset{x=y+1}{=} \chi(y^3 + y^2 - 1) = -1$.

V prípade S_{11}^{10} majú podmienky tvar

- $\chi(1 - y) = -1$,
- $\chi(x + 1 - y) \overset{x=y+1}{=} \chi(2) = 1$ (platí iba ak $q \equiv 1 \bmod 8$),
- $\chi(f_2(x, y)) \overset{x=y+1}{=} \chi(y^2 + 1) = 1$.

V prípade S_{00}^{01} majú podmienky tvar

- $\chi(1 - y) = -1$,
- $\chi(y + xy - x) \overset{x=y+1}{=} \chi(y^2 + y - 1) = 1$,
- $\chi(f_4(x, y)) \overset{x=y+1}{=} \chi(y^3 + y^2 - 1) = 1$.

V prípade S_{01}^{01} sa využíva $\eta = \chi(y + 1 - x)$, čo po dosadení za x dá nulu. Z čoho plynie, že by sa v každom prípade mali podmienky rovnať $\eta = 0$. Všetky 3 podmienky vedú v tomto prípade na

- $\chi(y^2 + y - 1) = 0$.

Kedže sa teda jedná len o y, ktoré sú koreňom polynómu y^2+y-1 a nás zaujímajú asymptotické odhady, môžeme týchto niekoľko málo y zanedbať.

V prípade S_{10}^{10} sa opäť využíva $\eta = \chi(x + 1 - y)$. Po dosadení za x však v tomto prípade dostávame

$$\eta = \chi(x + 1 - y) \overset{x=y+1}{=} \chi(2) = \begin{cases} 1, & \text{ak } q \equiv 1 \bmod 8, \\ -1, & \text{ak } q \equiv 5 \bmod 8. \end{cases}$$

Musíme teda rozlíšiť 2 situácie v závislosti na hodnote η. Obe situácie vedú na podmienky, ktoré sa líšia len o (-1) na pravej strane. Zapíšeme túto skutočnosť pomocou ± 1, kde horná hodnota reprezentuje situáciu $\eta = 1$. Podmienky sú teda

- $\chi(x+xy-y) \overset{x=y+1}{=} \chi(y^2+y+1) = \mp 1$,
- $\chi(g_2(x,y)) \overset{x=y+1}{=} \chi(y^2-y+1) = \mp 1$,
- $\chi(g_3(x,y)) \overset{x=y+1}{=} \chi(-y^2+y+1) = \pm 1$.

Spojením všetkých uvedených podmienok pre množiny S_{ij}^{rs} a rozlíšením na 2 situácie v závislosti na q mod 8 dostávame dané lemma.

□

2.2 Tvrdenie 1.27 pre prípad $t_1(x, y) = 0$

V tejto sekcii sa zameráme na Tvrdenie 1.27 a rovnako ako v predchádzajúcej sekcii uvedieme podmienky pre množiny S_{ij}^{rs}, ktoré musí spĺňať $(x,y) \in S$, aby $(x,y) \in S_{ij}^{rs}$, a to za dodatočnej podmienky, že je daný vzťah medzi x a y taký, že pre polynóm $t_1(x,y) = x-1-y$ platí $t_1(x,y) = 0$. Z čoho plynie $x = y+1$. V takom prípade budú polynómy uvedené v podmienkach iba v jednej neznámej y a na miesto dvojice (x,y) budeme písať $(y+1,y)$. Následne využijeme popisy množín S_{ij}^{rs} za uvedenej dodatočnej podmienky pre odhad veľkosti množiny T v sekciách 2.3.3 a 2.3.4.

Lemma 2.2. *Podmienky pre neprázdne množiny S_{ij}^{rs} uvedené v Tvrdení 1.27 majú v prípade dodatočnej podmienky $t_1(x,y) = 0$ tvar:*

- *V prípade $q \equiv 3 \bmod 8$ platí:*

$$\begin{aligned}
S_{01}^{00} = S_{01}^{11} = S_{11}^{01} = &S_{00}^{10} = S_{01}^{01} = \emptyset \\
(y+1,y) \in S_{01}^{10} &\iff \chi(y-1) = -1 \\
(y+1,y) \in S_{10}^{00} &\iff \chi(y-1) = 1 \ a \ \chi(-y^2+y-1) = -1 \\
(y+1,y) \in S_{01}^{11} &\iff \chi(y-1) = 1 \ a \ \chi(-y^2-y+1) = -1 \\
(y+1,y) \in S_{11}^{10} &\iff \chi(y-1) = \chi(-y^2-1) = 1 \\
(y+1,y) \in S_{00}^{01} &\iff \chi(y-1) = \chi(-y^2-y+1) = \chi(-y^3-y^2+1) = 1 \\
(y+1,y) \in S_{10}^{10} &\iff \chi(y^2+y+1) = \chi(-y^2+y-1) = \\
&\qquad = \chi(y^2-y-1) = -1
\end{aligned}$$

- *V prípade $q \equiv 7 \bmod 8$ platí:*

$$\begin{aligned}
S_{01}^{00} = S_{01}^{11} = S_{11}^{01} = &S_{00}^{10} = S_{01}^{01} = S_{11}^{10} = \emptyset \\
(y+1,y) \in S_{01}^{10} &\iff \chi(y-1) = -1 \\
(y+1,y) \in S_{10}^{00} &\iff \chi(y-1) = 1 \ a \ \chi(-y^2+y-1) = -1 \\
(y+1,y) \in S_{01}^{11} &\iff \chi(y-1) = 1 \ a \ \chi(-y^2-y+1) = -1 \\
(y+1,y) \in S_{00}^{01} &\iff \chi(y-1) = \chi(-y^2-y+1) = \chi(-y^3-y^2+1) = 1 \\
(y+1,y) \in S_{10}^{10} &\iff \chi(y^2+y+1) = \chi(-y^2+y-1) = \\
&\qquad = \chi(y^2-y-1) = 1
\end{aligned}$$

Dôkaz. Štruktúra dôkazu bude podobná ako v dôkaze Lemma 2.1.

V celom dôkaze budeme z predpokladov Tvrdenia 1.27 predpokladať, že je $q \equiv 3 \bmod 4$ (teda -1 nie je štvorec alebo tiež $\chi(-1) = -1$).

Do pôvodnej podoby tohto tvrdenia teda dosadíme $x = y + 1$ a určíme, ako vyzerajú jednotlivé podmienky pre množiny S_{ij}^{rs} využitím predpokladu $\chi(-1) = -1$ a ďalších vlastností kvadratického charakteru χ.

Množiny S_{01}^{00}, S_{10}^{11}, S_{11}^{01} a S_{00}^{10} sú prázdne, pretože podmienka $\chi((1-x)(x-y)) \overset{x=y+1}{=} \chi(-y) = 1$ nemá riešenie, keďže $\chi(-1) = -1$ a $\chi(y) = 1$.

Množina S_{01}^{01} je prázdna, pretože podmienka $\chi((x - xy - y)(x - 1 - y)) \overset{x=y+1}{=} \chi(0) = 1$ nemá riešenie, keďže z definície χ je $\chi(0) = 0$.

V prípade S_{01}^{10} majú podmienky tvar

- $\chi((1-y)(x-y)) \overset{x=y+1}{=} \chi(1-y) = 1$,
- $\chi((1-x)(y-x)) \overset{x=y+1}{=} \chi(y) = 1$ (platí vždy, predpokladáme $\chi(y) = 1$).

V prípade S_{10}^{00} majú podmienky tvar

- $\chi((1-y)(y-x)) \overset{x=y+1}{=} \chi(y-1) = 1$,
- $\chi(g_2(x,y)(x-y)) \overset{x=y+1}{=} \chi(y^2 - y + 1) = 1$.

V prípade S_{01}^{11} majú podmienky tvar

- $\chi((1-y)(y-x)) \overset{x=y+1}{=} \chi(y-1) = 1$,
- $\chi(g_4(x,y)(y-x)) \overset{x=y+1}{=} \chi(y^2 + y - 1) = 1$.

V prípade S_{11}^{10} majú podmienky tvar

- $\chi((1-y)(y-x)) \overset{x=y+1}{=} \chi(y-1) = 1$,
- $\chi(y - 1 - x) \overset{x=y+1}{=} \chi(-2) = 1$ (platí iba ak $q \equiv 3 \bmod 8$) ,
- $\chi((y-x)f_2(x,y)) \overset{x=y+1}{=} \chi(-y^2 - 1) = 1$.

V prípade S_{00}^{01} majú podmienky tvar

- $\chi((1-y)(y-x)) \overset{x=y+1}{=} \chi(y-1) = 1$,
- $\chi(x - xy - y) \overset{x=y+1}{=} \chi(-y^2 - y + 1) = 1$,
- $\chi((y-x)f_4(x,y)) \overset{x=y+1}{=} \chi(-y^3 - y^2 + 1) = 1$.

V prípade S_{10}^{10} majú podmienky tvar

- $\chi((y - xy - x)(y - 1 - x)) \overset{x=y+1}{=} \chi(2y^2 + 2y + 2) = 1$,
- $\chi(g_2(x,y)(x-y)(y-1-x)) \overset{x=y+1}{=} \chi(-2y^2 + 2y - 2) = 1$,
- $\chi(g_3(x,y)(x-y)(y-1-x)) \overset{x=y+1}{=} \chi(2y^2 - 2y - 2) = 1$.

V prípade $q \equiv 7 \bmod 8$ dodatočne využijeme $\chi(2) = 1$ v podmienkach množiny S_{10}^{10}, a v prípade $q \equiv 3 \bmod 8$ zas $\chi(2) = -1$.

Pre množiny S_{01}^{10}, S_{10}^{00} a S_{01}^{11} dodatočne využijeme predpoklad $\chi(-1) = -1$.

Spojením všetkých uvedených podmienok pre množiny S_{ij}^{rs} a rozlíšením na 2 prípady v závislosti na $q \bmod 8$ dostávame dané lemma.

□

2.3 Asymptotické odhady

V tejto časti práce uvedieme asymptotický odhad veľkosti množiny T na základe popisu množiny T^* uvedeného v sekcii 1.4. Tento asymptotický odhad následne využijeme pri určení pravdepodobnosti, s akou pri náhodnej voľbe $(y+1, y) \in S'$ padne $(y+1, y)$ do T. Pri dodatočnej podmienke $t_1(x, y) = 0$ je $S' = \{(x, y) \in S : x = y + 1\}$.

Dôležitou informáciou pre realizáciu asymptotického odhadu sú podmienky pre množiny S_{ij}^{rs} získané v Lemma 2.1 a v Lemma 2.2, ktoré vychádzali z Tvrdenia 1.26 a z Tvrdenia 1.27 pridaním dodatočného predpokladu $t_1(x, y) = 0$. V oboch prípadoch sa podmienky založené na polynómoch v x a y transformovali na podmienky s polynómami v jednej neznámej y. Vďaka tomu môžeme po dodatočných úvahách priamo aplikovať Vetu 1.6. Tieto podmienky sa v závislosti na q delia na 4 skupiny a to nasledovne

- $q \equiv 1 \bmod 8$,
- $q \equiv 5 \bmod 8$,
- $q \equiv 3 \bmod 8$,
- $q \equiv 7 \bmod 8$.

Prvé 2 prípady vychádzajú z Lemma 2.1 a v oboch prípadoch zároveň platí $q \equiv 1 \bmod 4$. Zvyšné prípady sú uvedené v Lemma 2.2 a v nich zároveň platí $q \equiv 3 \bmod 4$. Pre každý z týchto prípadov budeme musieť realizovať asymptotický odhad veľkosti množiny T samostatne. Postupne rozoberieme jednotlivé prípady vo zvyšku tejto sekcie.

Pozrime sa na veľkosť množiny S'. Zaujíma nás teda počet $y \in \mathbb{F}_q$ tak, že y aj $y + 1$ sú nenulové štvorce. Využijeme Vetu 1.4, podľa ktorej je to $\approx 1/4$ zo všetkých y. Keďže budeme pracovať s asymptotickými odhadmi, stačí nám približná veľkosť S', teda platí $\left|S'\right| \approx (q-1)/4$.

Na odhad veľkosti množiny T budeme používať Vetu 1.6. Predpoklady tejto vety však vyžadujú, aby bol zoznam polynómov bezštvorcový. Preto si zhrnieme zoznam polynómov, ktoré budeme v uvedených 4 prípadoch v závislosti na q potrebovať, a ukážeme, že je to naozaj bezštvorcový zoznam polynómov. V ďalšej časti sa už na toto lemma budeme len odkazovať.

Lemma 2.3. *Zoznam polynómov* y, $y+1$, $1-y$, y^2+1, y^2+y-1, y^2+y+1, y^2-y+1, $-y^2+y+1$, y^3-y-1 *a* y^3+y^2-1 *je bezštvorcový, ak platí* $\mathrm{char}(\mathbb{F}_q) > 5$.

Dôkaz. Je zrejmé, že lineárne polynómy majú navzájom rôzne korene v prípade, že $\mathrm{char}(\mathbb{F}_q) > 2$ a tiež žiaden z ostatných polynómov s nimi koreň nezdieľa. Preto sa môžeme zamerať už len na nelineárne polynómy.

Kvadratické polynómy y^2+1, y^2+y-1, y^2+y+1, y^2-y+1 a $-y^2+y+1$ majú korene v tomto poradí $\pm\sqrt{-4}/2$, $(-1\pm\sqrt{5})/2$, $(-1\pm\sqrt{-3})/2$, $(1\pm\sqrt{-3})/2$ a $(1\pm\sqrt{5})/2$. Z toho je vidno, že nezdieľajú koreň a pridaním predpokladu $\mathrm{char}(\mathbb{F}_q) > 5$ navyše nedôjde ani k tomu, aby jeden polynóm mal dvojnásobný koreň a teda by bol sám o sebe štvorcom.

Nakoniec sa pozrime na kubické polynómy $y^3 - y - 1$ a $y^3 + y^2 - 1$. Ich korene sú rôzne a za predpokladu $\mathrm{char}(\mathbb{F}_q) > 3$ sa vyhneme dvojnásobnému koreňu v oboch polynómoch. A platí tiež, že žiaden kvadratický polynóm nedelí kubické polynómy. Celkovo teda dostávame, že vynásobením ľubovoľných polynómov daného zoznamu nezískame štvorec a preto sa jedná o bezštvorcový zoznam polynómov. □

2.3.1 $q \equiv 1 \bmod 8$

V tejto sekcii je našim cieľom asymptotický odhad veľkosti množiny T^* za predpokladu $q \equiv 1 \bmod 8$. Následne tento asymptotický odhad využijeme k určeniu pravdepodobnosti, s akou náhodne zvolená dvojica $(y+1, y) \in S'$ padne do T.

Začnime tým, že pripomenieme podmienky z Lemma 2.1, ktoré musí spĺňať y, aby dvojica $(y+1, y) \in S'$ patrila do jednej z množín S_{ij}^{rs}.

$$
\begin{aligned}
&(y+1,y) \in S_{00}^{00} \iff \chi(1-y) = 1\\
&(y+1,y) \in S_{00}^{11} \iff \chi(y^3-y-1) = \chi(y^3+y^2-1) = -1\\
&(y+1,y) \in S_{11}^{10} \iff \chi(1-y) = -1 \text{ a } \chi(y^2+1) = 1\\
&(y+1,y) \in S_{00}^{01} \iff \chi(y^2+y-1) = \chi(y^3+y^2-1) = 1 \text{ a } \chi(1-y) = -1\\
&(y+1,y) \in S_{10}^{10} \iff \chi(y^2+y+1) = \chi(y^2-y+1) = -1 \text{ a } \chi(-y^2+y+1) = 1
\end{aligned}
$$

Okrem práve uvedených podmienok musí y z definície množiny S splňovať navyše $\chi(y) = \chi(y+1) = 1$. Tieto podmienky pridáme až na záver našich úvah. Sústreďme sa teraz na podmienky uvedené vyššie, pomocou ktorých popíšme množinu T^*.

Popíšme najprv jednotlivé množiny S_{ij}^{rs}. Preto si označme polynómy, ktoré sa v jednotlivých podmienkach vyskytujú takto

$$
\begin{aligned}
&p_1(y) = 1-y, && p_2(y) = y^3-y-1,\\
&p_3(y) = y^3+y^2-1, && p_4(y) = y^2+1,\\
&p_5(y) = y^2+y-1, && p_6(y) = y^2+y+1,\\
&p_7(y) = y^2-y+1, && p_8(y) = -y^2+y+1,\\
&p_9(y) = y \qquad \text{a} && p_{10}(y) = y+1.
\end{aligned}
$$

Tieto polynómy majú najviac 19 rôznych koreňov. Nás ale zaujíma asymptotický odhad, preto týchto niekoľko málo hodnôt y môžeme zanedbať a ďalej budeme predpokladať, že y nie je koreňom žiadneho z týchto polynómov.

Využijeme Označenie 1.28, ktoré musíme predefinovať pre našu konkrétnu situáciu a to tak, že $\langle p(y), \omega\rangle = \{(y+1, y) \in S^{'} : \chi(p(y)) = \omega\}$, pre $p(y) \in \mathbb{F}_q[y]$ a $\omega \in \{1, -1\}$. To využijeme tak, že pre $e \in \{1, \ldots, 8\}$ a polynóm $p_e(y)$ položíme

$$A_e = \langle p_e(y), 1\rangle \qquad \text{a} \qquad B_e = \langle p_e(y), -1\rangle. \tag{2.1}$$

V prípade $e \in \{9, 10\}$ definujeme A_e.

Keďže predpokladáme, že y nie je koreňom žiadneho z polynómov $p_e(y)$, zrejme platí $\overline{A_e} = B_e$.

Potom platí

$$\begin{aligned} S_{00}^{00} &= A_1, \\ S_{00}^{11} &= B_2 \cap B_3, \\ S_{11}^{10} &= B_1 \cap A_4, \\ S_{00}^{01} &= A_5 \cap A_3 \cap B_1, \\ S_{10}^{10} &= B_6 \cap B_7 \cap A_8. \end{aligned}$$

Ďalej budeme postupovať ako v obecnom prípade uvedenom v sekcii 1.4 na strane 13 a vyjadríme množinu T^* pomocou množín A_e a B_e.

Najprv musíme charakterizovať doplnky množín S_{ij}^{rs} v $S^{'}$, ktoré značíme $\overline{S_{ij}^{rs}}$. Platí

$$\begin{aligned} \overline{S_{00}^{00}} &= B_1, \\ \overline{S_{00}^{11}} &= A_2 \cup A_3, \\ \overline{S_{11}^{10}} &= A_1 \cup B_4, \\ \overline{S_{00}^{01}} &= B_5 \cup B_3 \cup A_1, \\ \overline{S_{10}^{10}} &= A_6 \cup A_7 \cup B_8. \end{aligned}$$

Ako je uvedené v (1.13), je množina T^* prienikom týchto množín $\overline{S_{ij}^{rs}}$. Platí

$$\begin{aligned} T^* &= B_1 \cap (A_2 \cup A_3) \cap (A_1 \cup B_4) \cap (B_5 \cup B_3 \cup A_1) \cap (A_6 \cup A_7 \cup B_8) = \\ &= B_1 \cap (A_2 \cup A_3) \cap B_4 \cap (B_5 \cup B_3) \cap (A_6 \cup A_7 \cup B_8). \end{aligned}$$

Množinu T^* však potrebujeme zapísať ako zjednotenie disjunktných množín. Vyššie uvedený výraz rozoberieme po častiach. Využívame, že $A \cup B = (\overline{A} \cap B) \cup (A \cap \overline{B}) \cup (A \cap B)$ je vyjadrenie zjednotenia dvoch množín pomocou zjednotenia disjunktných množín. Potom je vidno, že pre $(A_2 \cup A_3) \cap (B_5 \cup B_3)$ platí

$$\begin{aligned} (A_2 \cup A_3) \cap (B_5 \cup B_3) =& (A_2 \cap B_3 \cap B_5) \cup (B_2 \cap A_3 \cap B_5) \cup \\ & (A_2 \cap A_3 \cap B_5) \cup (A_2 \cap B_3 \cap A_5), \end{aligned}$$

kde 4 množiny na pravej strane sú navzájom disjunktné.

Pre výraz $A_6 \cup A_7 \cup B_8$ platí

$$\begin{aligned} (A_6 \cup A_7 \cup B_8) =& (A_6 \cap A_7 \cap A_8) \cup (A_6 \cap A_7 \cap B_8) \cup (A_6 \cap B_7 \cap A_8) \cup \\ & (A_6 \cap B_7 \cap B_8) \cup (B_6 \cap A_7 \cap A_8) \cup (B_6 \cap A_7 \cap B_8) \cup \\ & (B_6 \cap B_7 \cap B_8), \end{aligned}$$

kde opäť platí, že množiny na pravej strane sú disjunktné.

Celkovo teda dostávame, že množinu T^* vieme zapísať ako zjednotenie 28 disjunktných množín, kde pre každú z týchto množín musíme kvôli asymptotickým odhadom pridať ešte podmienku $\chi(y) = \chi(y+1) = 1$ čo je ekvivalentné tomu, že pre každú množinu tvoriacu disjunktný rozklad T^* pridáme do prieniku množín množiny A_9 a A_{10}. Preto každá z 28 disjunktných množín je určená práve 10 polynómami a v každom prípade ide o polynómy, ktorých súčet stupňov je práve 19. Zoznam týchto disjunktných množín je uvedený v Tabuľke A.1, ktorá sa nachádza v prílohe tejto práce.

Konečne sme pripravení pristúpiť k samotnému asymptotického odhadu veľkosti T^*, ktorý uvedieme v nasledujúcom tvrdení.

Tvrdenie 2.4. *Predpokladajme $q \equiv 1 \bmod 8$, $q > 5$. Pre náhodne zvolené $(a,b) \in \Sigma$ také, že $(a,b) = \Psi^{-1}((x,y))$, kde x a y spĺňajú: $(x,y) \in S$ a $t_1(x,y) = 0$, je $Q_{a,b}$ maximálne neasociatívna kvázigrupa s pravdepodobnosťou $\approx 0{,}109$. Navyše platí, že maximálne neasociatívna kvázigrupa $Q_{a,b}$ spĺňajúca tieto podmienky vždy existuje pre $q > 594\,423$ a pre prvočíselné $q \leq 594\,423$ taká kvázigrupa existuje práve vtedy $q \geq 41$ a zároveň $q \neq 97$.*

Dôkaz. Dôkaz začneme odhadom asymptotickej veľkosti množiny T^*. Z diskusie pred týmto tvrdením plynie, že množinu T^* vieme zapísať ako zjednotenie 28 navzájom disjunktných množín. Preto Vetu 1.6 aplikujeme na každú z týchto množín samostatne a jednotlivé odhady sčítame.

Najprv overíme, že sú splnené predpoklady Vety 1.6. Polynómy, ktoré budeme vo vete využívať sú práve polynómy $p_1(y), \ldots, p_{10}(y)$. Z Lemma 2.3 plynie, že sa jedná o bezštvorcový zoznam polynómov, čím je predpoklad vety splnený.

Ako sme už uviedli pri analýze tohto prípadu, v zozname týchto polynómov môže byť maximálne 19 rôznych koreňov. Keďže nás zaujíma asymptotický odhad, môžeme týchto niekoľko hodnôt y zanedbať. Preto pridaním členu s hodnotou 19 do nášho odhadu môžeme ďalej predpokladať, že y nie je koreňom žiadneho z týchto polynómov.

Teraz už môžeme aplikovať Vetu 1.6 a dostávame

$$\begin{aligned}
\left| |T^*| - \Big(\sum_{j=1}^{28} 2^{-k_j}\Big) q \right| &< (\sqrt{q}+1)\Big(\sum_{j=1}^{28} D_j\Big)/2 + 19, \\
\left| |T^*| - 28 \cdot 2^{-10} q \right| &< (\sqrt{q}+1)(28 \cdot 19)/2 + 19, \\
\left| |T^*| - 28 \cdot 2^{-10} q \right| &< (\sqrt{q}+1)266 + 19. \qquad (2.2)
\end{aligned}$$

Z toho je vidno, že

$$\lim_{q \to \infty} \frac{|T^*|}{q} = \frac{28}{2^{10}} \doteq 0{,}0273.$$

Ako sme uviedli na začiatku sekcie 2.3, platí $\left|S'\right| \approx (q-1)/4$. V spojení s asymptotickým odhadom veľkosti množiny T^* je zrejmé, že pri náhodnej voľbe y, ktoré spĺňuje $(y+1, y) \in S'$, padne dvojica $(y+1, y)$ do T^* s pravdepodobnosťou približne 0,109.

Pripomeňme, že pre $(a,b) \in \Sigma$ platí $(a,b) = \Psi^{-1}((x,y))$, kde Ψ je bijekcia definovaná vzťahom (1.7) a $(x,y) \in S$. Z čoho je zrejme vidieť, že práve uvedená pravdepodobnosť je totožná s pravdepodobnosťou v znení tvrdenia.

Ostáva ukázať, že pre každé q existuje maximálne neasociatívna kvázigrupa $Q_{a,b}$, ktorá spĺňuje predpoklady tvrdenia. Využijeme vzťah (2.2) a dostávame, že taká maximálne neasociatívna kvázigrupa určite existuje, ak platí

$$28 \cdot 2^{-10} q > (\sqrt{q} + 1)266 + 19. \tag{2.3}$$

To platí práve vtedy, keď $q > 94\,654\,828$. Aby sme túto hodnotu znížili, môžeme tento dôkaz existencie urobiť pre nejakú podmnožinu T^*, ktorá je popísaná menším počtom podmienok. Za takú podmnožinu T^* môžeme zvoliť množinu $B_1 \cap A_3 \cap B_4 \cap B_5 \cap A_6 \cap A_9 \cap A_{10}$, označme ju U. Ide o množinu danú 7 polynómami so súčtom stupňov 12. Na zoznam tých 7 polynómov, ktoré nám dávajú U aplikujeme Vetu 1.6 a urobíme rovnaký trik ako pri dôkaze existencie pre celé T^*. Dostávame, že pre $(x,y) \in U$ existuje maximálne neasociatívna kvázigrupa $Q_{a,b}$ práve vtedy, keď

$$2^{-7} q > (\sqrt{q} + 1)6 + 12,$$

čo platí práve vtedy, keď $q > 594\,423$. Zrejme teda platí, že pre $q > 594\,423$ existuje taká kvázigrupa pre $(x,y) \in T^*$.

Pre prvočíselné $q \leq 594\,423$ sme experimentálne overili, že taká kvázigrupa existuje práve vtedy, keď $q \geq 41$ a zároveň $q \neq 97$.

□

Pravdepodobnosť uvedenú v predchádzajúcom tvrdení sme ešte dodatočne experimentálne overili výpočtom skutočnej veľkosti množiny T^*, pre všetky prvočísla $q \equiv 1 \bmod 8$ a $q < 100\,000$, za danej dodatočnej podmienky. Použili sme na to Algoritmus 6, ktorý je uvedený v Kapitole 5. Výsledok tohto overenia je uvedený v grafe na Obrázku B.1 v prílohe tejto práce. Experimentálne overenie zrejme naznačuje správnosť našich výpočtov.

Na experimentálne overenie existencie maximálne neasociatívnej kvázigrupy na záver dôkazu Tvrdenia 2.4 sme využili Algoritmus 7, ktorý je tiež uvedený v Kapitole 5.

2.3.2 $q \equiv 5 \bmod 8$

V tejto sekcii je opäť našim cieľom asymptotický odhad veľkosti množiny T^*. Tentokrát za predpokladu $q \equiv 5 \bmod 8$. Rovnako ako v predchádzajúcej sekcii ho využijeme k určeniu pravdepodobnosti, s akou náhodne zvolená dvojica $(y+1, y) \in S'$ padne do T.

Keďže je postup v tomto prípade takmer identický s tým, ktorý sme použili v predchádzajúcej sekcii pre prípad $q \equiv 1 \bmod 8$, budeme v tejto sekcii a tiež v prípadoch $q \equiv 3 \bmod 8$ a $q \equiv 7 \bmod 8$ postupovať len veľmi stručne, pretože detailný popis postupu si čitateľ môže prečítať pri riešení prípadu $q \equiv 1 \bmod 8$.

V tomto prípade pre úplný zoznam podmienok, ktoré musí spĺňať y, aby dvojica $(y+1,y)$ patrila do jednej z množín S_{ij}^{rs} odkážeme čitateľa na Lemma 2.1.

V tomto prípade tieto podmienky pracujú s polynómami

$$\begin{aligned} p_1(y) &= 1 - y, & p_2(y) &= y^3 - y - 1, \\ p_3(y) &= y^3 + y^2 - 1, & p_4(y) &= y^2 + y - 1, \\ p_5(y) &= y^2 + y + 1, & p_6(y) &= y^2 - y + 1, \\ p_7(y) &= -y^2 + y + 1, & p_8(y) &= y \text{ a} \\ p_9(y) &= y + 1. \end{aligned}$$

Opäť definujeme množiny A_e a B_e rovnako ako v sekcii 2.3.1 vzťahom (2.1). Pomocou množín A_e a B_e môžeme zapísať množiny S_{ij}^{rs} a $\overline{S_{ij}^{rs}}$. Platí

$$\begin{aligned} S_{00}^{00} &= A_1, & \overline{S_{00}^{00}} &= B_1, \\ S_{00}^{11} &= B_2 \cap B_3, & \overline{S_{00}^{11}} &= A_2 \cup A_3, \\ S_{00}^{01} &= A_4 \cap A_3 \cap B_1, & \overline{S_{00}^{01}} &= B_4 \cup B_3 \cup A_1, \\ S_{10}^{10} &= A_5 \cap A_6 \cap B_7, & \overline{S_{10}^{10}} &= B_5 \cup B_6 \cup A_7. \end{aligned}$$

Opäť vychádzame z obecného popisu množiny T^* daného vzťahom (1.13) a preto

$$T^* = B_1 \cap (A_2 \cup A_3) \cap (B_4 \cup B_3) \cap (B_5 \cup B_6 \cup A_7).$$

Tvar množiny T^* je takmer rovnaký ako v prípade $q \equiv 1 \bmod 8$ a líši sa len v tom, že v predchádzajúcom prípade bola v tomto prieniku uvedená ešte jedna množina navyše, ktorá bola daná polynómom stupňa 2. Okrem toho je rozdiel už len v tom, že na miesto výrazu $(A_6 \cup A_7 \cup B_8)$ sa v tomto prípade pracuje s $(B_5 \cup B_6 \cup A_7)$, kde sa však využívajú rovnaké polynómy. Preto môžeme vychádzať z výsledkov predchádzajúcej sekcie, a teda dostávame, že v tomto prípade sa dá T^* zapísať ako zjednotenie 28 disjunktných množín, kde každá z týchto množín je daná práve 9 polynómami a v každom príde je súčet stupňov týchto polynómov 17. Zoznam všetkých disjunktných množín je uvedený v Tabuľke A.2, ktorá sa nachádza v prílohe tejto práce.

Tvrdenie 2.5. *Predpokladajme $q \equiv 5 \bmod 8$, $q > 5$. Pre náhodne zvolené $(a, b) \in \Sigma$ také, že $(a, b) = \Psi^{-1}((x, y))$, kde x a y splňujú: $(x, y) \in S$ a $t_1(x, y) = 0$, je $Q_{a,b}$ maximálne neasociatívna kvázigrupa s pravdepodobnosťou $\approx 0{,}219$. Navyše platí, že maximálne neasociatívna kvázigrupa $Q_{a,b}$ splňujúca tieto podmienky vždy existuje pre $q > 104\,311$ a pre prvočíselné $q \leq 104\,311$ taká kvázigrupa existuje práve vtedy $q \geq 13$.*

Dôkaz. Dôkaz má identickú štruktúru ako dôkaz Tvrdenia 2.4 a preto už v tomto prípade nebudeme zachádzať do všetkých detailov, ktoré si čitateľ môže prečítať v dôkaze odkazovaného tvrdenia.

Rovnako ako v Tvrdení 2.4 vychádzame z toho, že množinu T^* vieme zapísať, ako zjednotenie 28 disjunktných množín, kde každá z týchto množín je daná práve 9 polynómami a v každom príde je súčet stupňov týchto polynómov 17.

V tomto prípade však pracujeme s polynómami $p_1(y), \ldots, p_9(y)$. Z Lemma 2.3 plynie, že ide o bezštvorcový zoznam polynómov, čím je predpoklad Vety 1.6 splnený. V tomto zozname polynómov môže byť maximálne 17 rôznych koreňov. Preto aj v tomto prípade môžeme tieto y zanedbať.

Teraz už môžeme aplikovať Vetu 1.6 a dostávame

$$\left||T^*| - 28 \cdot 2^{-9}q\right| < (\sqrt{q}+1)238 + 17. \tag{2.4}$$

Z toho je vidno, že

$$\lim_{q\to\infty} \frac{|T^*|}{q} \doteq 0{,}05469.$$

Aj v tomto prípade pracujeme s množinou S', ktorá splňuje $\left|S'\right| \approx (q-1)/4$. V spojení s asymptotickým odhadom veľkosti množiny T^* je zrejmé, že hľadaná pravdepodobnosť je približne 0,2188.

Využijeme vzťah (2.4) a dostávame, že maximálne neasociatívna kvázigrupa $Q_{a,b}$ existuje, ak platí

$$28 \cdot 2^{-9}q > (\sqrt{q}+1)238 + 17.$$

To platí práve vtedy, keď $q > 18\,949\,228$. Aj v tomto prípade, sa dá táto hodnota znížiť tak, že ako podmnožinu T^* si vezmeme množinu $U = B_1 \cap A_3 \cap B_4 \cap B_5 \cap A_8 \cap A_9$, ktorá je daná 6 polynómami so súčtom stupňov 10. Na zoznam tých polynómov aplikujeme Vetu 1.6 a dostávame, že pre $(x, y) \in U$ existuje maximálne neasociatívna kvázigrupa $Q_{a,b}$ práve vtedy, keď

$$2^{-6}q > (\sqrt{q}+1)5 + 10,$$

čo platí práve vtedy, keď $q > 104\,311$. Zrejme teda platí, že pre $q > 104\,311$ taká kvázigrupa existuje pre $(x, y) \in T^*$.

Pre prvočíselné $q \leq 104\,311$ sme experimentálne overili, že taká kvázigrupa existuje práve vtedy, keď $q \geq 13$.

□

Rovnako aj v tomto prípade sme pravdepodobnosť uvedenú v predchádzajúcom tvrdení dodatočne experimentálne overili výpočtom skutočnej veľkosti množiny T^*. V tomto prípade je výsledok tohto overenia uvedený v grafe, ktorý je uvedený na Obrázku B.2 v prílohe tejto práce. Experimentálne overenie zrejme naznačuje správnosť našich výpočtov.

Na experimentálne overenie existencie maximálne neasociatívnej kvázigrupy na záver dôkazu Tvrdenia 2.5 sme opäť využili Algoritmus 7.

2.3.3 $q \equiv 3 \bmod 8$

Opäť je našim cieľom asymptotický odhad veľkosti množiny T^*, tentokrát za predpokladu $q \equiv 3 \bmod 8$. Ten využijeme k určeniu pravdepodobnosti, s akou náhodne zvolená dvojica $(y+1, y) \in S'$ padne do T. Opäť budeme postupovať stručnejšie ako v prípade $q \equiv 1 \bmod 8$, kde je daný postup podobný, ale podrobnejšie vysvetlený.

Úplný zoznam podmienok, ktoré musí spĺňať y, aby dvojica $(y+1,y)$ patrila do jednej z množín S_{ij}^{rs} je uvedený v Lemma 2.2.

V tomto prípade tieto podmienky pracujú s polynómami

$$\begin{aligned} p_1(y) &= y-1, & p_2(y) &= -y^2+y-1,\\ p_3(y) &= -y^2-y+1, & p_4(y) &= -y^2-1,\\ p_5(y) &= -y^3-y^2+1, & p_6(y) &= y^2+y+1,\\ p_7(y) &= y^2-y-1, & p_8(y) &= y \text{ a}\\ p_9(y) &= y+1. \end{aligned}$$

Opäť definujeme množiny A_e a B_e rovnako ako v sekcii 2.3.1 vzťahom (2.1). Pomocou množín A_e a B_e môžeme zapísať množiny S_{ij}^{rs} a $\overline{S_{ij}^{rs}}$ takto:

$$\begin{aligned} S_{01}^{10} &= B_1, & \overline{S_{01}^{10}} &= A_1,\\ S_{10}^{00} &= A_1 \cap B_2, & \overline{S_{10}^{00}} &= B_1 \cup A_2,\\ S_{01}^{11} &= A_1 \cap B_3, & \overline{S_{01}^{11}} &= B_1 \cup A_3,\\ S_{11}^{10} &= A_1 \cap A_4, & \overline{S_{11}^{10}} &= B_1 \cup B_4,\\ S_{00}^{01} &= A_1 \cap A_3 \cap A_5, & \overline{S_{00}^{01}} &= B_1 \cup B_3 \cup B_5,\\ S_{10}^{10} &= B_6 \cap B_2 \cap B_7, & \overline{S_{10}^{10}} &= A_6 \cup A_2 \cup A_7. \end{aligned}$$

Opäť vychádzame z obecného popisu množiny T^* daného vzťahom (1.13). Platí

$$T^* = A_1 \cap A_2 \cap A_3 \cap B_4 \cap B_5 \cap (A_6 \cup A_2 \cup A_7).$$

Všimnime si, že platí

$$\begin{aligned} A_2 \cap (A_6 \cup A_2 \cup A_7) =& (A_2 \cap A_6 \cap A_7) \cup (A_2 \cap B_6 \cap A_7) \cup \\ & (A_2 \cap B_6 \cap B_7) \cup (A_2 \cap A_6 \cap B_7) \end{aligned}$$

a zjednotenie výrazov na pravej strane nám dáva jedinú obmädzujúcu podmienku v podobne množiny A_2, keďže $(A_6 \cap A_7) \cup (B_6 \cap A_7) \cup (B_6 \cap B_7) \cup (A_6 \cap B_7)$ nam dáva celú množinu S.

Z toho plynie, že v skutočnosti platí

$$T^* = A_1 \cap A_2 \cap A_3 \cap B_4 \cap B_5.$$

a teda popis množiny T^* je po pridaní $A_8 \cap A_9$ daný 7 polynómami, ktorých súčet stupňov je 12. Pre úplnosť prílohy je aj v tomto prípade v prílohe uvedená Tabuľka A.3, kde je táto množina uvedená rovnakým spôsobom ako v ostatných prípadoch.

Tvrdenie 2.6. *Predpokladajme $q \equiv 3 \bmod 8$, $q > 5$. Pre náhodne zvolené $(a,b) \in \Sigma$ také, že $(a,b) = \Psi^{-1}((x,y))$, kde x a y splňujú: $(x,y) \in S$ a $t_1(x,y) = 0$, je $Q_{a,b}$ maximálne neasociatívna kvázigrupa s pravdepodobnosťou $\approx 0{,}031$. Navyše platí, že maximálne neasociatívna kvázigrupa $Q_{a,b}$ splňujúca tieto podmienky vždy existuje pre $q > 594\,423$ a navyše pre prvočíselné $q \leq 594\,423$ taká kvázigrupa existuje práve vtedy, keď $q \geq 19$ a zároveň $q \notin \{43, 67, 83, 131\}$.*

Dôkaz. Dôkaz má identickú štruktúru ako dôkaz Tvrdenia 2.4 a preto už v tomto prípade nebudeme zachádzať do všetkých detailov, ktoré si čitateľ môže prečítať v dôkaze odkazovaného tvrdenia.

Vychádzame z popisu množiny $T^* = A_1 \cap A_2 \cap A_3 \cap B_4 \cap B_5 \cap A_8 \cap A_9$ daného 7 polynómami, ktorých súčet stupňov je 12. V tomto prípade pracujeme s polynómami $p_1(y), \ldots, p_9(y)$. Z Lemma 2.3 plynie, že sa jedná o bezštvorcový zoznam polynómov, čím je predpoklad Vety 1.6 splnený. V tomto zozname polynómov môže byť maximálne 12 rôznych koreňov. Preto aj v tomto prípade môžeme tieto y zanedbať.

Teraz už môžeme aplikovať Vetu 1.6 a dostávame

$$\left||T^*| - 2^{-7}q\right| < (\sqrt{q}+1)6 + 12. \tag{2.5}$$

Z toho je vidno, že

$$\lim_{q\to\infty} \frac{|T^*|}{q} \doteq 0{,}0078.$$

Opäť platí $\left|S'\right| \approx (q-1)/4$. V spojení s asymptotickým odhadom veľkosti množiny T^* je zrejmé, že hľadaná pravdepodobnosť je približne 0,031.

Využijeme vzťah (2.5) a dostávame, že maximálne neasociatívna kvázigrupa $Q_{a,b}$ existuje, ak platí

$$2^{-7}q > (\sqrt{q}+1)6 + 12.$$

To platí práve vtedy, keď $q > 594\,423$. Pre prvočíselné $q \leq 594\,423$ sme experimentálne overili, že taká kvázigrupa existuje práve vtedy, keď pre $q \geq 19$ a zároveň $q \notin \{43, 67, 83, 131\}$.

□

Rovnako aj v tomto prípade sme pravdepodobnosť uvedenú v predchádzajúcom tvrdení dodatočne experimentálne overili výpočtom skutočnej veľkosti množiny T^*. V tomto prípade je výsledok tohto overenia uvedený v grafe, ktorý je uvedený na Obrázku B.3 v prílohe tejto práce. Experimentálne overenie zrejme naznačuje správnosť našich výpočtov.

Experimentálne overenie existencie maximálne neasociatívnej kvázigrupy $Q_{a,b}$ pre menšie prvočíselné hodnoty, než tie získane z asymptotického odhadu veľkosti T^* sme v dôkaze predchádzajúceho tvrdenia realizovali pomocou Algoritmu 7, uvedeného v Kapitole 5.

2.3.4 $q \equiv 7 \bmod 8$

Opäť je našim cieľom asymptotický odhad veľkosti množiny T^*, tentokrát za predpokladu $q \equiv 7 \bmod 8$. Ten využijeme k určeniu pravdepodobnosti, s akou náhodne zvolená dvojica $(y+1, y) \in S'$ padne do T.

Úplný zoznam podmienok, ktoré musí spĺňať y, aby dvojica $(y+1,y)$ patrila do jednej z množín S_{ij}^{rs} je uvedený v Lemma 2.2.

V tomto prípade tieto podmienky pracujú s polynómami

$$\begin{aligned} p_1(y) &= y-1, & p_2(y) &= -y^2+y-1,\\ p_3(y) &= -y^2-y+1, & p_4(y) &= -y^3-y^2+1,\\ p_5(y) &= y^2+y+1, & p_6(y) &= y^2-y-1,\\ p_7(y) &= y \quad \text{a} & p_8(y) &= y+1. \end{aligned}$$

Opäť definujeme množiny A_e a B_e rovnako ako v sekcii 2.3.1 vzťahom (2.1). Pomocou množín A_e a B_e môžeme zapísať množiny S_{ij}^{rs} a $\overline{S_{ij}^{rs}}$ takto:

$$\begin{aligned} S_{01}^{10} &= B_1, & \overline{S_{01}^{10}} &= A_1,\\ S_{10}^{00} &= A_1 \cap B_2, & \overline{S_{10}^{00}} &= B_1 \cup A_2,\\ S_{01}^{11} &= A_1 \cap B_3, & \overline{S_{01}^{11}} &= B_1 \cup A_3,\\ S_{00}^{01} &= A_1 \cap A_3 \cap A_4, & \overline{S_{00}^{01}} &= B_1 \cup B_3 \cup B_4,\\ S_{10}^{10} &= A_5 \cap A_2 \cap A_6, & \overline{S_{10}^{10}} &= B_5 \cup B_2 \cup B_6. \end{aligned}$$

Opäť vychádzame z obecného popisu množiny T^* daného vzťahom (1.13). Platí

$$T^* = A_1 \cap A_2 \cap A_3 \cap B_4 \cap (B_5 \cup B_6).$$

Opäť využime, že platí $A \cup B = (\overline{A} \cap B) \cup (A \cap \overline{B}) \cup (A \cap B)$, vďaka čomu je vidno, že $(B_5 \cup B_6) = (A_5 \cap B_6) \cup (B_5 \cap A_6) \cup (B_5 \cap B_6)$ a teda množinu T^* môžeme zapísať ako zjednotenie 3 disjunktných množín. Každá z 3 množín je daná 8 polynómami so súčtom stupňov 14. Zoznam týchto disjunktných množín je aj v tomto prípade uvedený v Tabuľke A.4, ktorá sa nachádza v prílohe tejto práce.

Tvrdenie 2.7. *Predpokladajme $q \equiv 7 \bmod 8$, $q > 5$. Pre náhodne zvolené $(a,b) \in \Sigma$ také, že $(a,b) = \Psi^{-1}((x,y))$, kde x a y spĺňajú: $(x,y) \in S$ a $t_1(x,y) = 0$, je $Q_{a,b}$ maximálne neasociatívna kvázigrupa s pravdepodobnosťou $\approx 0{,}047$. Navyše platí, že maximálne neasociatívna kvázigrupa $Q_{a,b}$ spĺňajúca tieto podmienky vždy existuje pre $q > 594\,423$ a pre prvočíselné $q \leq 594\,423$ taká kvázigrupa existuje práve vtedy, keď $q \geq 23$ a zároveň $q \notin \{31, 47, 239\}$.*

Dôkaz. Dôkaz má identickú štruktúru ako dôkaz Tvrdenia 2.4 a preto už v tomto prípade nebudeme zachádzať do všetkých detailov, ktoré si čitateľ môže prečítať v dôkaze odkazovaného tvrdenia.

Vychádzame z popisu množiny T^* ako sme ho uviedli pred týmto tvrdením. V tomto prípade pracujeme s polynómami $p_1(y), \ldots, p_8(y)$. Z Lemma 2.3 plynie, že sa jedná o bezštvorcový zoznam polynómov, čím je predpoklad Vety 1.6 splnený. V tomto zozname polynómov môže byť maximálne 14 rôznych koreňov. Preto aj v tomto prípade môžeme tieto y zanedbať.

Aplikujeme Vetu 1.6 a dostávame

$$\left| |T^*| - 3 \cdot 2^{-8} q \right| < (\sqrt{q}+1)21 + 14. \tag{2.6}$$

Z toho je vidno, že

$$\lim_{q\to\infty} \frac{|T^*|}{q} \doteq 0{,}0117.$$

Opäť platí $\left|S'\right| \approx (q-1)/4$. V spojení s asymptotickým odhadom veľkosti množiny T^* je zrejmé, že hľadaná pravdepodobnosť je približne 0,047.

Využijeme vzťah (2.6) a dostávame, že maximálne neasociatívna kvázigrupa $Q_{a,b}$ existuje, ak platí

$$3 \cdot 2^{-8} q > (\sqrt{q}+1)21 + 14.$$

To platí práve vtedy, keď $q > 3\,217\,234$. Aj v tomto prípade, sa dá táto hodnota znížiť tak, že ako podmnožinu T^* si vezmeme množinu $U = A_1 \cap A_2 \cap A_3 \cap B_4 \cap B_5 \cap A_7 \cap A_8$, ktorá je daná 7 polynómami so súčtom stupňov 12. Na zoznam tých polynómov aplikujeme Vetu 1.6 a dostávame, že pre $(x, y) \in U$ existuje maximálne neasociatívna kvázigrupa $Q_{a,b}$ práve vtedy, keď

$$2^{-7} q > (\sqrt{q}+1)6 + 12,$$

čo platí práve vtedy, keď $q > 594\,423$. Zrejme teda platí, že pre $q > 594\,423$ taká kvázigrupa existuje pre $(x, y) \in T^*$.

Pre prvočíselné $q \leq 594\,423$ sme experimentálne overili, že taká kvázigrupa existuje práve vtedy, keď $q \geq 23$ a zároveň $q \notin \{31, 47, 239\}$.

□

Rovnako aj v tomto prípade sme pravdepodobnosť uvedenú v predchádzajúcom tvrdení dodatočne experimentálne overili výpočtom skutočnej veľkosti množiny T^*. V tomto prípade je výsledok tohto overenia uvedený v grafe, ktorý je uvedený na Obrázku B.4 v prílohe tejto práce. Experimentálne overenie zrejme naznačuje správnosť našich výpočtov.

Na experimentálne overenie existencie maximálne neasociatívnej kvázigrupy na záver dôkazu Tvrdenia 2.7 sme opäť využili Algoritmus 7.

3. $f_1(x, y) = 0$

Oproti prípadu $t_1(x, y) = 0$ musíme vynaložiť o čosi viac úsilia, pretože nejde vyjadriť x ako funkciu y a zrejme ani opačne. Prichádza tu však do úvahy určitá transformácia, pomocou ktorej už budeme môcť vyjadriť jednu neznámu ako funkciu druhej neznámej. Ak by sme totiž položili

$$d = y/x \text{ a } h = x^{-1} \tag{3.1}$$

tak po vydelení $f_1(x, y)$ polynómom x^2 dostávame

$$f_1(x, y)/x^2 = d^2 - d - h + 1$$

čo po dosadení do podmienky $f_1(x, y) = 0$ dáva vzťah

$$h = d^2 - d + 1.$$

Aby mohol byť náš postup v prípade predpokladu $f_1(x, y) = 0$ podobný s tým, aký sme použili pri prípade využívajúcom predpoklad $t_1(x, y) = 0$ musíme transformáciu danú vzťahom (3.1) aplikovať aj na Tvrdenie 1.26 a Tvrdenie 1.27. Až následne budeme schopní tieto tvrdenia uviesť v podobe, ktorá využíva uvedený dodatočný predpoklad. Táto podoba tvrdení nám potom umožní počítať asymptotický odhad veľkosti množiny T^*.

Aby sme túto transformáciu mohli aplikovať, musíme najprv všetky polynómy v týchto tvrdeniach vydeliť najnižšou mocninou x, ktorá nám umožní celý výraz nahradiť pomocou d a h. To môžeme urobiť pretože pre ľubovoľný polynóm $p(x,y)$ platí $\chi(p(x,y)) = \chi(p(x,y)/x)$ a to vďaka tomu, že pracujeme v telese, v ktorom pre nenulové x platí: x je štvorec práve vtedy, keď x^{-1} je štvorec. Vďaka tomu navyše platí $\chi(d) = \chi(h) = 1$, keďže predpokladáme x^{-1} aj y štvorce. Tieto skutočnosti budeme v ďalšej časti často využívať.

3.1 Tvrdenie 1.26 pre prípad $f_1(x, y) = 0$

V tejto sekcii sa zameráme na Tvrdenie 1.26 a uvedieme podmienky pre množiny S_{ij}^{rs}, ktoré musí spĺňať $(x, y) \in S$, aby $(x, y) \in S_{ij}^{rs}$, a to za dodatočnej podmienky, že je daný vzťah medzi x a y taký, že pre polynóm $f_1(x, y) = x^2 + y^2 - xy - x$ platí $f_1(x, y) = 0$.

Aby sme to mohli urobiť, najprv uvedieme podobu Tvrdenia 1.26 po aplikovaní transformácie danej vzťahom (3.1).

Lemma 3.1. *Podmienky pre neprázdne množiny S_{ij}^{rs} v Tvrdení 1.26 majú po vydelení polynómov v týchto podmienkach mocninou x, ktorá odpovedá súčtu mocnín x a y v tom člene polynómu, ktorý má tento súčet najvyšší, a následnou transformáciou využitím vzťahu* (3.1) *tvar:*

Platí $d = y/x$ a $h = x^{-1}$. Položme $\varepsilon = \chi(1-d)$. Potom

$$
\begin{aligned}
(x,y) \in S_{00}^{00} &\iff \chi(h-1) = \chi(h-d) = \varepsilon,\\
(x,y) \in S_{11}^{00} &\iff \chi(d^2-d-h+1) = \chi(d^2-d-dh+1) = -\varepsilon,\\
(x,y) \in S_{00}^{11} &\iff \chi(d^2+dh-h-d^2h) = \chi(d+dh-h-d^2h) = -\varepsilon,\\
(x,y) \in S_{11}^{01} &\iff \chi(h-1) = -\varepsilon, \chi(d+h-1) = 1 \text{ a } \chi(d^2-d-h+1) = \varepsilon,\\
(x,y) \in S_{11}^{10} &\iff \chi(h-d) = -\varepsilon, \chi(1+h-d) = 1 \text{ a } \chi(d^2-d-dh+1) = \varepsilon,\\
(x,y) \in S_{00}^{10} &\iff \chi(h-1) = -\varepsilon, \chi(h+d-hd) = 1 \text{ a } \chi(d^2+dh-h-d^2h) = \varepsilon,\\
(x,y) \in S_{00}^{01} &\iff \chi(h-d) = -\varepsilon, \chi(dh+d-h) = 1 \text{ a } \chi(d+dh-h-d^2h) = \varepsilon,\\
(x,y) \in S_{01}^{01} &\iff \chi(dh+d-h) = -\eta, \chi(1+dh-2h) = -\eta\varepsilon \text{ a}\\
&\qquad \chi(d^2+h-2d) = \eta\varepsilon, \text{kde } \eta = \chi(d+h-1),\\
(x,y) \in S_{10}^{10} &\iff \chi(h+d-hd) = -\eta, \chi(d^2+h-2dh) = -\eta\varepsilon \text{ a}\\
&\qquad \chi(1+dh-2d) = \eta\varepsilon, \text{kde } \eta = \chi(1+h-d).
\end{aligned}
$$

Ďalej teda budeme predpokladať, že platí $h = d^2-d+1$. Pri tomto predpoklade budú polynómy uvedené v podmienkach iba v jednej neznámej d.

Lemma 3.2. *Podmienky pre neprázdne množiny S_{ij}^{rs} uvedené v Tvrdení 1.26 majú v prípade dodatočnej podmienky $f_1(x,y) = 0$, ktorá sa po transformácii danej vzťahom* (3.1) *dá tiež zapísať ako $h = d^2-d+1$, tvar:*

$$
\begin{aligned}
S_{11}^{00} = S_{11}^{01} = S_{00}^{10} = S_{01}^{01} &= \emptyset,\\
(x,y) \in S_{00}^{00} &\iff \chi(1-d) = 1,\\
(x,y) \in S_{00}^{11} &\iff \chi((1-d)(d^2+1)) = \chi(d^3-d^2+2d-1) = -1,\\
(x,y) \in S_{11}^{10} &\iff \chi(1-d) = -1 \text{ a } \chi(d^2-2d+2) = 1,\\
(x,y) \in S_{00}^{01} &\iff \chi(1-d) = -1, \chi(d^3-2d^2+3d-1) = 1 \text{ a}\\
&\qquad \chi(d^3-d^2+2d-1) = 1,\\
(x,y) \in S_{10}^{10} &\iff \chi((d^2-2d+2)(-d^3+2d^2-d+1)) = -1,\\
&\qquad \chi((d^2-2d+2)(2d^2-2d+1)) = -1 \text{ a}\\
&\qquad \chi((d^2-2d+2)(d+1)(1-d)) = 1,
\end{aligned}
$$

kde vzťah medzi x, y a d, h je daný práve vzťahom (3.1).

Dôkaz. Tvrdenie 1.26 predpokladá $q \equiv 1 \bmod 4$, teda platí $\chi(-1) = 1$, a to budeme v celom dôkaze predpokladať.

V tomto prípade budeme vychádzať z podmienok uvedených v Lemma 3.1, ktoré je odvodené z Tvrdenia 1.26 tak, ako sme to popísali vyššie. Ďalej toto Lemma uvádza $\varepsilon = \chi(1-d)$. Do podoby tohto tvrdenia v Lemma 3.1 teda dosadíme $h = d^2-d+1$ a $\varepsilon = \chi(1-d)$ a určíme, ako vyzerajú jednotlivé podmienky pre množiny S_{ij}^{rs} využitím predpokladu $\chi(-1) = 1$ a ďalších vlastností kvadratického charakteru χ.

Pri zápise jednotlivých podmienok využijeme symbol $\overset{?}{=}$ tak, že na ľavej strane tohto symbolu bude uvedená hodnota χ určitého polynómu v danej podmienke a na pravej strane symbolu $\overset{?}{=}$ bude výraz, ktorému sa musí výraz na ľavej strane rovnať, aby bola podmienka splnená.

U množín S_{11}^{00} a S_{11}^{01} by podmienka $\chi(d^2-d-h+1) \stackrel{?}{=} \pm\varepsilon$ viedla na $0 \stackrel{?}{=} \pm\chi(1-d)$. Keďže však predpokladáme x aj y rôzne od 1, musí byť aj $d \neq 1$ a preto táto podmienka nemá riešenie a obe množiny sú v tomto prípade prázdne.

Množina S_{00}^{10} je prázdna, pretože podmienka $\chi(h-1) \stackrel{?}{=} -\varepsilon$ vedie na $\chi((d-1)d) = \chi(d-1) \stackrel{?}{=} -\chi(1-d)$ čo opäť za predpokladu $d \neq 1$ nemá riešenie.

U prípadu S_{01}^{01} sa definuje $\eta = \chi(d+h-1) \stackrel{h=d^2-d+1}{=} \chi(d^2) = 1$. Podmienka $\chi(1+dh-2h) \stackrel{?}{=} -\eta\varepsilon$ má po dosadení tvar $\chi((d-1)^3) = \chi(d-1) \stackrel{?}{=} -\chi(1-d)$ čo opäť nemá žiadne riešenie, preto je množina S_{01}^{01} prázdna.

V prípade S_{00}^{00} majú podmienky po dosadení za h a ε tvar

- $\chi(h-1) \stackrel{h=d^2-d+1}{=} \chi((d-1)d) = \chi(d-1) \stackrel{?}{=} \chi(1-d)$ (platí vždy, pretože predpokladáme $\chi(-1)=1$),
- $\chi(h-d) \stackrel{h=d^2-d+1}{=} \chi((d-1)^2) = 1 \stackrel{?}{=} \chi(1-d)$.

V prípade S_{00}^{11} majú podmienky tvar

- $\chi(d^2+dh-h-d^2h) \stackrel{h=d^2-d+1}{=} \chi(-(d-1)^2(d^2+1)) = \chi(d^2+1) \stackrel{?}{=} -\chi(1-d)$, čo sa dá zapísať ako $\chi((1-d)(d^2+1)) \stackrel{?}{=} -1$,
- $\chi(d+dh-h-d^2h) \stackrel{h=d^2-d+1}{=} \chi(-(d-1)(d^3-d^2+2d-1)) \stackrel{?}{=} -\chi(1-d)$, čo sa dá zapísať ako $\chi((d-1)^2(d^3-d^2+2d-1)) = \chi(d^3-d^2+2d-1) \stackrel{?}{=} -1$.

V prípade S_{11}^{10} majú podmienky tvar

- $\chi(h-d) \stackrel{h=d^2-d+1}{=} \chi((d-1)^2) = 1 \stackrel{?}{=} -\chi(1-d)$, čo sa dá zapísať ako $\chi(1-d) \stackrel{?}{=} -1$,
- $\chi(1+h-d) \stackrel{h=d^2-d+1}{=} \chi(d^2-2d+2) \stackrel{?}{=} 1$,
- $\chi(d^2-d-dh+1) \stackrel{h=d^2-d+1}{=} \chi(-(d-1)(d^2-d+1)) \stackrel{?}{=} \chi(1-d)$, čo sa dá zapísať ako $\chi((d-1)^2(d^2-d+1)) = \chi(d^2-d+1) \stackrel{?}{=} 1$, čo zrejme platí vždy, keďže $h = d^2-d+1$ a predpokladáme h štvorec.

V prípade S_{00}^{01} majú podmienky tvar

- Rovnako ako u S_{11}^{10}: $\chi(1-d) \stackrel{?}{=} -1$,
- $\chi(dh+d-h) \stackrel{h=d^2-d+1}{=} \chi(d^3-2d^2+3d-1) \stackrel{?}{=} 1$,
- Rovnako ako 2. podmienka u S_{00}^{11} až na pravú stranu: $\chi(d^3-d^2+2d-1) \stackrel{?}{=} 1$.

V prípade S_{10}^{10} sa definuje $\eta = \chi(1+h-d)$, čo po dosadení za h dáva $\chi(d^2-2d+2)$. Potom podmienky majú tvar

- $\chi(h+d-hd) \stackrel{h=d^2-d+1}{=} \chi(-d^3+2d^2-d+1) \stackrel{?}{=} -\chi(d^2-2d+2)$, čo sa dá zapísať ako $\chi((d^2-2d+2)(-d^3+2d^2-d+1)) \stackrel{?}{=} -1$,

- $\chi(d^2+h-2dh) \overset{h=d^2-d+1}{=} \chi(-(d-1)(2d^2-2d+1)) \overset{?}{=} -\chi((1-d)(d^2-2d+2))$, čo sa dá zapísať ako $\chi((d-1)^2(2d^2-2d+1)(d^2-2d+2)) = \chi((2d^2-2d+1)(d^2-2d+2)) \overset{?}{=} -1$

- $\chi(1+dh-2d) \overset{h=d^2-d+1}{=} \chi((d-1)^2(d+1)) = \chi(d+1) \overset{?}{=} \chi((1-d)(d^2-2d+2))$, čo sa dá zapísať ako $\chi((d+1)(1-d)(d^2-2d+2)) \overset{?}{=} 1$.

Spojením všetkých uvedených podmienok pre množiny S_{ij}^{rs} dostávame dané lemma.

□

3.2 Tvrdenie 1.27 pre prípad $f_1(x, y) = 0$

V tejto sekcii sa zameráme na Tvrdenie 1.27 a uvedieme podmienky pre množiny S_{ij}^{rs}, ktoré musí spĺňať $(x, y) \in S$, aby $(x, y) \in S_{ij}^{rs}$, a to za dodatočnej podmienky, že je daný vzťah medzi x a y taký, že pre polynóm $f_1(x, y) = x^2 + y^2 - xy - x$ platí $f_1(x, y) = 0$.

Podobne ako v predchádzajúcej sekcii aj tu najprv uvedieme podobu Tvrdenia 1.27 po aplikovaní transformácie danej vzťahom (3.1).

Lemma 3.3. *Podmienky pre neprázdne množiny S_{ij}^{rs} v Tvrdení 1.27 majú po vydelení polynómov v týchto podmienkach mocninou x, ktorá odpovedá súčtu mocnín x a y v tom člene polynómu, ktorý má tento súčet najvyšší, a následnou transformáciou využitím vzťahu* (3.1) *tvar:*

Platí $d = y/x$ a $h = x^{-1}$. Potom

$$\begin{aligned}
(x,y) \in S_{01}^{10} &\iff \chi((h-d)(1-d)) = \chi((h-1)(d-1)) = 1,\\
(x,y) \in S_{01}^{00} &\iff \chi((h-1)(1-d)) = \chi((1+dh-2h)(d-1)) = 1,\\
(x,y) \in S_{10}^{00} &\iff \chi((h-d)(d-1)) = \chi((d^2+h-2dh)(1-d)) = 1,\\
(x,y) \in S_{10}^{11} &\iff \chi((h-1)(1-d)) = \chi((1+dh-2d)(1-d)) = 1,\\
(x,y) \in S_{01}^{11} &\iff \chi((h-d)(d-1)) = \chi((d^2+h-2d)(d-1)) = 1,\\
(x,y) \in S_{11}^{01} &\iff \chi((h-1)(1-d)) = \chi(1-h-d) =\\
&\qquad = \chi((1-d)(d^2-d-h+1)) = 1,\\
(x,y) \in S_{11}^{10} &\iff \chi((h-d)(d-1)) = \chi(d-h-1) =\\
&\qquad = \chi((d-1)(d^2+1-d-dh)) = 1,\\
(x,y) \in S_{00}^{10} &\iff \chi((h-1)(1-d)) = \chi(dh-d-h) =\\
&\qquad = \chi((1-d)(d^2+dh-h-d^2h)) = 1,\\
(x,y) \in S_{00}^{01} &\iff \chi((h-d)(d-1)) = \chi(h-d-dh) =\\
&\qquad = \chi((d-1)(d+dh-h-d^2h)) = 1,\\
(x,y) \in S_{01}^{01} &\iff \chi((h-d-dh)(1-h-d)) =\\
&\qquad = \chi((1+dh-2h)(d-1)(1-h-d)) =\\
&\qquad = \chi((d^2+h-2d)(d-1)(1-h-d)) = 1,\\
(x,y) \in S_{10}^{10} &\iff \chi((dh-d-h)(d-h-1)) =\\
&\qquad = \chi((d^2+h-2dh)(1-d)(d-h-1)) =\\
&\qquad = \chi((1+dh-2d)(1-d)(d-h-1)) = 1.
\end{aligned}$$

Ďalej teda budeme predpokladať, že platí $h = d^2-d+1$. Pri tomto predpoklade budú polynómy uvedené v podmienkach iba v jednej neznámej d.

Lemma 3.4. *Podmienky pre neprázdne množiny S_{ij}^{rs} uvedené v Tvrdení 1.27 majú v prípade dodatočnej podmienky $f_1(x,y) = 0$, ktorá sa po transformácii danej vzťahom* (3.1) *dá tiež zapísať ako $h = d^2 - d + 1$, tvar:*

$$\begin{aligned}
S_{01}^{00} = S_{10}^{11} = S_{11}^{01} = S_{00}^{10} = S_{01}^{01} = S_{11}^{10} &= \emptyset,\\
(x,y) \in S_{01}^{10} &\iff \chi(d-1) = -1,\\
(x,y) \in S_{10}^{00} &\iff \chi(d-1) = \chi(2d^2-2d+1) = 1,\\
(x,y) \in S_{01}^{11} &\iff \chi(d-1) = \chi(2d-1) = 1,\\
(x,y) \in S_{00}^{01} &\iff \chi(d-1) = \chi(-d^3+2d^2-3d+1) =\\
&\qquad = \chi(-d^3+d^2-2d+1) = 1,\\
(x,y) \in S_{10}^{10} &\iff \chi((d^2-2d+2)(d^3-2d^2+d-1)) = -1,\\
&\qquad \chi((d^2-2d+2)(2d^2-2d+1)) = -1 \text{ a}\\
&\qquad \chi((d^2-2d+2)(d+1)(d-1)) = 1,
\end{aligned}$$

kde vzťah medzi x, y a d, h je daný práve vzťahom (3.1).

Dôkaz. Tvrdenie 1.27 predpokladá $q \equiv 3 \bmod 4$, teda platí $\chi(-1) = -1$, a to budeme v celom dôkaze predpokladať.

V tomto prípade budeme vychádzať z podmienok uvedených v Lemma 3.3, ktoré je odvodené z Tvrdenia 1.27 tak, ako sme to popísali vyššie. Do podoby tohto

tvrdenia v Lemma 3.3 dosadíme $h = d^2 - d + 1$ a určíme, ako vyzerajú jednotlivé podmienky pre množiny S_{ij}^{rs} využitím predpokladu $\chi(-1) = 1$ a ďalších vlastností kvadratického charakteru χ.

Pri zápise jednotlivých podmienok využijeme symbol $\stackrel{?}{=}$ tak, že na ľavej strane tohto symbolu bude uvedená hodnota χ určitého polynómu v danej podmienke a na pravej strane symbolu $\stackrel{?}{=}$ bude výraz, ktorému sa musí výraz na ľavej strane rovnať, aby bola podmienka splnená.

Množiny S_{01}^{00}, S_{10}^{11}, S_{11}^{01} a S_{00}^{10} sú prázdne, pretože podmienka $\chi((h-1)(1-d)) \stackrel{h=d^2-d+1}{=} \chi(-d(d-1)^2) = \chi(-1) \stackrel{?}{=} 1$ zrejme nie je splnená nikdy za predpokladu $\chi(-1) = -1$.

Množina S_{01}^{01} je prázdna, pretože podmienka $\chi((1+dh-2h)(d-1)(1-h-d)) \stackrel{h=d^2-d+1}{=} \chi(-(d-1)^4 d^2) \stackrel{?}{=} 1$ zrejme neplatí za žiadných okolností.

Množina S_{11}^{10} je prázdna, pretože podmienka $\chi((d-1)(d^2+1-d-dh)) \stackrel{h=d^2-d+1}{=} \chi(-(d-1)^2(d^2-d+1)) = \chi(-(d^2-d+1)) \stackrel{?}{=} 1$ zrejme nemá riešenie, keďže $h = d^2 - d + 1$ a predpokladáme h štvorec.

V prípade S_{01}^{10} majú podmienky po dosadení za h tvar

- $\chi((h-d)(1-d)) \stackrel{h=d^2-d+1}{=} \chi(-(d-1)^3) = \chi(-(d-1)) \stackrel{?}{=} 1$, čo sa dá zapísať ako $\chi(d-1) \stackrel{?}{=} -1$,
- $\chi((h-1)(d-1)) \stackrel{h=d^2-d+1}{=} \chi(d(d-1)^2) \stackrel{?}{=} 1$, čo zrejme platí vždy.

V prípade S_{10}^{00} majú podmienky tvar

- $\chi((h-d)(d-1)) \stackrel{h=d^2-d+1}{=} \chi((d-1)^3) = \chi(d-1) \stackrel{?}{=} 1$,
- $\chi((d^2+h-2dh)(1-d)) \stackrel{h=d^2-d+1}{=} \chi((d-1)^2(2d^2-2d+1)) = \chi(2d^2-2d+1) \stackrel{?}{=} 1$.

V prípade S_{01}^{11} majú podmienky tvar

- Rovnako ako u S_{10}^{00}: $\chi(d-1) \stackrel{?}{=} 1$,
- $\chi((d^2+h-2d)(d-1)) \stackrel{h=d^2-d+1}{=} \chi((d-1)^2(2d-1)) = \chi(2d-1) \stackrel{?}{=} 1$.

V prípade S_{00}^{01} majú podmienky tvar

- Rovnako ako u S_{10}^{00}: $\chi(d-1) \stackrel{?}{=} 1$,
- $\chi(h-d-dh) \stackrel{h=d^2-d+1}{=} \chi(-d^3+2d^2-3d+1) \stackrel{?}{=} 1$,
- $\chi((d-1)(d+dh-h-d^2h)) \stackrel{h=d^2-d+1}{=} \chi(-(d-1)^2(d^3-d^2+2d-1)) = \chi(-d^3+d^2-2d+1) \stackrel{?}{=} 1$.

V prípade S_{10}^{10} majú podmienky tvar

- $\chi((dh-d-h)(d-h-1)) \stackrel{h=d^2-d+1}{=} \chi(-(d^2-2d+2)(d^3-2d^2+d-1)) \stackrel{?}{=} 1$, čo sa dá zapísať ako $\chi((d^2-2d+2)(d^3-2d^2+d-1)) \stackrel{?}{=} -1$,

- $\chi((d^2+h-2dh)(1-d)(d-h-1)) \overset{h=d^2-d+1}{=} \chi(-(d-1)^2(d^2-2d+2)(2d^2-2d+1)) = \chi(-(d^2-2d+2)(2d^2-2d+1)) \overset{?}{=} 1$, čo sa dá zapísať ako $\chi((d^2-2d+2)(2d^2-2d+1)) \overset{?}{=} -1$,
- $\chi((1+dh-2d)(1-d)(d-h-1)) \overset{h=d^2-d+1}{=} \chi((d-1)^3(d+1)(d^2-2d+2)) = \chi((d-1)(d+1)(d^2-2d+2)) \overset{?}{=} 1$.

Spojením všetkých uvedených podmienok pre množiny S_{ij}^{rs} dostávame dané lemma.

□

3.3 Asymptotické odhady

V tejto časti práce uvedieme asymptotický odhad veľkosti množiny T na základe popisu množiny T^* uvedeného v sekcii 1.4, a to za podmienky $f_1(x,y)=0$. Tento asymptotický odhad následne využijeme pri určení pravdepodobnosti, s akou pri náhodnej voľbe $(x,y) \in S'$ padne dvojica (x,y) do T. Pri dodatočnej podmienke $f_1(x,y)=0$ je $S' = \{(x,y) \in S : h = d^2-d+1$, kde $d = y/x$ a $h = x^{-1}\}$.

Dôležitou informáciou pre realizáciu asymptotického odhadu sú podmienky pre množiny S_{ij}^{rs} získané v Lemma 3.2 a v Lemma 3.4, ktoré vychádzali z Tvrdenia 1.26 a z Tvrdenia 1.27 pridaním dodatočného predpokladu $f_1(x,y)=0$. V oboch prípadoch sa podmienky založené na polynómoch v d a h transformovali na podmienky s polynómami v jednej neznámej d. Vďaka tomu môžeme aj v tomto prípade po dodatočných úvahách priamo aplikovať Vetu 1.6. Podmienky sa v závislosti na q delia v tomto prípade len na 2 prípady

- $q \equiv 1 \bmod 4$,
- $q \equiv 3 \bmod 4$.

Pre oba prípady teda musíme realizovať asymptotický odhad veľkosti množiny T^* samostatne, čo urobíme vo zvyšku tejto kapitoly.

Pozrime sa na veľkosť množiny S'. V tomto prípade nás zaujíma počet $d \in \mathbb{F}_q$ tak, že d aj d^2-d+1 sú štvorce. Táto požiadavka zároveň zaručuje, že x a y budú štvorce. Z Vety 1.6 plynie, že d aj d^2-d+1 sú štvorce s pravdepodobnosťou $\approx 1/4$, preto $\left|S'\right| \approx (q-1)/4$.

Na odhad veľkosti množiny T^* budeme používať Vetu 1.6. Predpoklady tejto vety však vyžadujú, aby bol zoznam polynómov bezštvorcový. Preto si zhrnieme zoznam polynómov, ktoré budeme v uvedených 2 prípadoch v závislosti na q potrebovať a ukážeme, že je to naozaj bezštvorcový zoznam. V ďalšej časti sa už na toto lemma budeme len odkazovať.

Lemma 3.5. *Zoznam polynómov* d, $1-d$, $d+1$, $2d-1$, d^2-d+1, d^2+1, d^2-2d+2, $2d^2-2d+1$, d^3-d^2+2d-1, d^3-2d^2+3d-1 *a* $-d^3+2d^2-d+1$ *je bezštvorcový, ak platí* $\mathrm{char}(\mathbb{F}_q) > 5$.

Dôkaz. Je zrejmé, že lineárne polynómy majú navzájom rôzne korene v prípade, že $\mathrm{char}(\mathbb{F}_q) > 3$ a žiaden z kvadratických polynómov s nimi koreň nezdieľa ak $\mathrm{char}(\mathbb{F}_q) > 5$.

Kvadratické polynómy d^2-d+1, d^2+1, d^2-2d+2 a $2d^2-2d+1$ majú korene v tomto poradí $(1\pm\sqrt{-3})/2$, $\pm\sqrt{-1}$, $1\pm\sqrt{-1}$ a $(1\pm\sqrt{-1})/2$. Z toho je vidno, že za predpokladu $\mathrm{char}(\mathbb{F}_q)>5$ nezdieľajú koreň a tiež žiaden polynóm nemá dvojnásobný koreň.

Nakoniec sa pozrime na kubické polynómy d^3-d^2+2d-1, d^3-2d^2+3d-1 a $-d^3+2d^2-d+1$. Ich korene sú rôzne a za predpokladu $\mathrm{char}(\mathbb{F}_q)>5$ sa vyhneme dvojnásobnému koreňu v daných polynómoch. A platí tiež, že žiaden lineárny ani kvadratický polynóm nedelí kubické polynómy.

Celkovo teda dostávame, že vynásobením ľubovoľných polynómov daného zoznamu nezískame štvorec a preto sa jedná o bezštvorcový zoznam polynómov.

□

3.3.1 $q \equiv 1 \bmod 4$

V tejto sekcii je našim cieľom asymptotický odhad veľkosti množiny T^* za predpokladu $q\equiv 1 \bmod 4$, ktorý použijeme k určeniu pravdepodobnosti, s akou náhodne zvolená dvojica $(x,y)\in S'$ padne do T.

Podobne ako vo všetkých skúmaných prípadoch v tejto práci, aj v tomto prípade vychádzame pri asymptotickom odhade veľkosti množiny T^* z podmienok na náležanie dvojice $(x,y)\in S'$ do jednej z množín S_{ij}^{rs}, ktoré sú pre tento konkrétny prípad uvedené v Lemma 3.2.

Okrem podmienok zo spomenutého Lemma musíme pre asymptotické odhady doplniť podmienky z definície množiny S, ktoré vzhľadom na použitie transformácie danej vzťahom (3.1) vyžadujú, aby d aj $h=d^2-d+1$ boli štvorce, čo sa dá zapísať ako $\chi(d)=\chi(d^2-d+1)=1$. Tieto podmienky pridáme až na záver našich úvah a teraz sa sústredíme na podmienky z Lemma 3.2, pomocou ktorých popíšeme množinu T^*.

Označme si polynómy, ktoré sa v jednotlivých podmienkach vyskytujú, takto

$$\begin{aligned}
&p_1(d)=1-d, && p_2(d)=d^2+1,\\
&p_3(d)=d^3-d^2+2d-1, && p_4(d)=d^2-2d+2,\\
&p_5(d)=d^3-2d^2+3d-1, && p_6(d)=-d^3+2d^2-d+1,\\
&p_7(d)=2d^2-2d+1, && p_8(d)=d+1,\\
&p_9(d)=d \qquad \text{a} && p_{10}(d)=d^2-d+1.
\end{aligned}$$

Tieto polynómy majú najviac 20 rôznych koreňov. Nás ale zaujíma asymptotický odhad, preto týchto niekoľko málo hodnôt d môžeme zanedbať a ďalej budeme predpokladať, že d nie je koreňom žiadneho z týchto polynómov.

Využijeme Označenie 1.28, ktoré musíme predefinovať pre našu konkrétnu situáciu a to tak, že $\langle p(d),\omega\rangle=\{(x,y)\in S' : \chi(p(d))=\omega, \text{ kde } d=y/x\}$, pre $p(d)\in\mathbb{F}_q[d]$ a $\omega\in\{1,-1\}$. To využijeme tak, že pre $e\in\{1,\dots,8\}$ a polynóm $p_e(d)$ položíme

$$A_e=\langle p_e(d),1\rangle \qquad \text{a} \qquad B_e=\langle p_e(d),-1\rangle. \tag{3.2}$$

V prípade $e\in\{9,10\}$ definujeme týmto spôsobom A_e.

Keďže predpokladáme, že d nie je koreňom žiadneho z polynómov $p_e(d)$, zrejme platí $\overline{A_e}=B_e$, čo budeme využívať.

Budeme postupovať ako v obecnom prípade uvedenom v sekcii 1.4 na strane 13 a vyjadríme množinu T^* pomocou množín A_e a B_e. Preto potrebujeme pomocou množín A_e a B_e zapísať najprv množiny S_{ij}^{rs} a $\overline{S_{ij}^{rs}}$. Platí

$$\begin{aligned}
S_{00}^{00} =& A_1,\\
S_{00}^{11} =& ((B_1 \cap A_2) \cup (A_1 \cap B_2)) \cap B_3,\\
S_{11}^{10} =& B_1 \cap A_4,\\
S_{00}^{01} =& B_1 \cap A_5 \cap A_3,\\
S_{10}^{10} =& ((B_4 \cap A_6) \cup (A_4 \cap B_6)) \cap ((B_4 \cap A_7) \cup (A_4 \cap B_7)) \cap\\
& ((A_4 \cap A_8 \cap A_1) \cup (A_4 \cap B_8 \cap B_1) \cup (B_4 \cap B_8 \cap A_1) \cup (B_4 \cap A_8 \cap B_1)).
\end{aligned}$$

$$\begin{aligned}
\overline{S_{00}^{00}} =& B_1,\\
\overline{S_{00}^{11}} =& ((A_1 \cup B_2) \cap (B_1 \cup A_2)) \cup A_3,\\
\overline{S_{11}^{10}} =& A_1 \cup B_4,\\
\overline{S_{00}^{01}} =& A_1 \cup B_5 \cup B_3,\\
\overline{S_{10}^{10}} =& ((A_4 \cup B_6) \cap (B_4 \cup A_6)) \cup ((A_4 \cup B_7) \cap (B_4 \cup A_7)) \cup\\
& ((B_4 \cup B_8 \cup B_1) \cap (B_4 \cup A_8 \cup A_1) \cap (A_4 \cup A_8 \cup B_1) \cap (A_4 \cup B_8 \cup A_1)).
\end{aligned}$$

Ako je uvedené v (1.13), je množina T^* prienikom týchto množín $\overline{S_{ij}^{rs}}$. Platí

$$\begin{aligned}
T^* =& B_1 \cap (((A_1 \cup B_2) \cap (B_1 \cup A_2)) \cup A_3) \cap (A_1 \cup B_4) \cap\\
& (A_1 \cup B_5 \cup B_3) \cap (((A_4 \cup B_6) \cap (B_4 \cup A_6)) \cup ((A_4 \cup B_7) \cap (B_4 \cup A_7))) \cup\\
& ((B_4 \cup B_8 \cup B_1) \cap (B_4 \cup A_8 \cup A_1) \cap (A_4 \cup A_8 \cup B_1) \cap (A_4 \cup B_8 \cup A_1))).
\end{aligned}$$

Množinu T^* však potrebujeme zapísať ako zjednotenie disjunktných množín. Pri úprave výrazu využijeme skutočnosť, že pre množiny A a B platí

$$(A \cup \overline{B}) \cap (\overline{A} \cup B) = (A \cap B) \cup (\overline{A} \cap \overline{B}). \tag{3.3}$$

Potom zrejme platí

$$\begin{aligned}
T^* =& B_1 \cap ((A_1 \cap A_2) \cup (B_1 \cap B_2) \cup A_3) \cap B_4 \cap (B_5 \cup B_3) \cap\\
& ((A_4 \cap A_6) \cup (B_4 \cap B_6) \cup (A_4 \cap A_7) \cup (B_4 \cap B_7) \cup B_8)\\
=& B_1 \cap B_4 \cap ((B_1 \cap B_2) \cup A_3) \cap (B_5 \cup B_3) \cap ((B_4 \cap (B_6 \cup B_7)) \cup B_8)\\
=& B_1 \cap B_4 \cap (B_2 \cup A_3) \cap (B_5 \cup B_3) \cap (B_6 \cup B_7 \cup B_8).
\end{aligned}$$

A ďalej využijeme, že vzťah

$$A \cup B = (\overline{A} \cap B) \cup (A \cap \overline{B}) \cup (A \cap B) \tag{3.4}$$

je vyjadrenie zjednotenia množín A a B pomocou zjednotenia disjunktných množín. Potom je vidno, že pre $(B_2 \cup A_3) \cap (B_5 \cup B_3)$ platí

$$\begin{aligned}
(B_2 \cup A_3) \cap (B_5 \cup B_3) =& (B_2 \cap B_3 \cap B_5) \cup (A_2 \cap A_3 \cap B_5) \cup\\
& (B_2 \cap A_3 \cap B_5) \cup (B_2 \cap B_3 \cap A_5),
\end{aligned}$$

kde 4 množiny na pravej strane sú navzájom disjunktné a každá je daná 3 polynómami.

Pre výraz $B_6 \cup B_7 \cup B_8$ platí

$$\begin{aligned}(B_6 \cup B_7 \cup B_8) =&(B_6 \cap B_7 \cap A_8) \cup (A_6 \cap A_7 \cap B_8) \cup (A_6 \cap B_7 \cap A_8) \cup \\ &(A_6 \cap B_7 \cap B_8) \cup (B_6 \cap A_7 \cap A_8) \cup (B_6 \cap A_7 \cap B_8) \cup \\ &(B_6 \cap B_7 \cap B_8),\end{aligned}$$

kde opäť platí, že množiny na pravej strane sú disjunktné.

Celkovo teda dostávame, že množinu T^* môžeme zapísať ako zjednotenie $4 \cdot 7 = 28$ disjunktných množín, kde pre každú z týchto množín musíme kvôli asymptotickým odhadom pridať ešte podmienku $\chi(d) = \chi(d^2 - d + 1) = 1$ čo je ekvivalentné tomu, že do prieniku množín u každej z 28 disjunktných množín pridáme množiny A_9 a A_{10}. Preto sú všetky disjunktné množiny, ktorých zjednotenie dáva T^*, dané 10 polynómami $p_1(d), \ldots, p_{10}(d)$ so súčtom stupňov 20. Zoznam všetkých disjunktných množín je uvedený v Tabuľke A.5, ktorá sa nachádza v prílohe tejto práce.

Konečne sme pripravení pristúpiť k samotnému asymptotického odhadu veľkosti T^*, ktorý uvedieme v nasledujúcom tvrdení.

Tvrdenie 3.6. *Predpokladajme $q \equiv 1 \bmod 4$, $q > 5$. Pre náhodne zvolené $(a, b) \in \Sigma$ také, že $(a, b) = \Psi^{-1}((x, y))$, kde x a y spĺňajú: $(x, y) \in S$ a $f_1(x, y) = 0$, je $Q_{a,b}$ maximálne neasociatívna kvázigrupa s pravdepodobnosťou $\approx 0{,}109$. Navyše platí, že maximálne neasociatívna kvázigrupa $Q_{a,b}$ spĺňajúca tieto podmienky vždy existuje pre $q > 594\,423$ a pre prvočíselné $q \leq 594\,423$ taká kvázigrupa existuje práve vtedy $q \geq 13$ a zároveň $q \notin \{17, 29, 53\}$.*

Dôkaz. Dôkaz začneme odhadom asymptotickej veľkosti množiny T^*. Z diskusie pred týmto tvrdením plynie, že množinu T^* vieme zapísať ako zjednotenie 28 navzájom disjunktných množín. Preto Vetu 1.6 aplikujeme na každú z týchto množín samostatne a jednotlivé odhady sčítame.

Najprv overíme, že sú splnené predpoklady Vety 1.6. Polynómy, ktoré budeme vo vete využívať sú práve polynómy $p_1(d), \ldots, p_{10}(d)$. Z Lemma 4.3 plynie, že sa jedná o bezštvorcový zoznam polynómov, čím je predpoklad vety splnený.

V zozname týchto polynómov môže byť najviac 20 rôznych koreňov. Keďže nás zaujíma asymptotický odhad, môžeme týchto niekoľko hodnôt d zanedbať. Preto pridaním členu s hodnotou 20 do nášho odhadu môžeme predpokladať, že d nie je koreňom žiadneho z týchto polynómov.

Teraz už môžeme aplikovať Vetu 1.6 a dostávame

$$\left| |T^*| - 28 \cdot 2^{-10} q \right| < (\sqrt{q} + 1)280 + 20. \tag{3.5}$$

Z toho je vidno, že

$$\lim_{q \to \infty} \frac{|T^*|}{q} \doteq 0{,}0273.$$

Ako sme uviedli na začiatku sekcie 3.3, platí $\left|S'\right| \approx (q-1)/4$. V spojení s asymptotickým odhadom veľkosti množiny T^* je zrejmé, že hľadaná pravdepodobnosť je približne 0,109.

Využijeme vzťah (3.5) a dostávame, že maximálne neasociatívna kvázigrupa $Q_{a,b}$ existuje, ak platí

$$28 \cdot 2^{-10} q > (\sqrt{q} + 1)280 + 20.$$

To platí práve vtedy, keď $q > 104\,879\,542$. Aby sme túto hodnotu znížili, môžeme tento dôkaz existencie urobiť pre nejakú podmnožinu T^*, ktorá je popísaná menším počtom podmienok. Za takú podmnožinu T^* môžeme zvoliť množinu $B_1 \cap B_2 \cap B_3 \cap B_4 \cap B_8 \cap A_9 \cap A_{10}$, ktorú označme U. Ide o množinu danú 7 polynómami so súčtom stupňov 12. Na zoznam tých 7 polynómov, ktoré nám dávajú U, aplikujeme Vetu 1.6 a urobíme rovnaký trik ako pri dôkaze existencie pre celé T^*. Dostávame, že pre $(x, y) \in U$ existuje maximálne neasociatívna kvázigrupa $Q_{a,b}$ práve vtedy, keď

$$2^{-7} q > (\sqrt{q} + 1)6 + 12,$$

čo platí práve vtedy, keď $q > 594\,423$. Zrejme teda platí, že pre $q > 594\,423$ existuje taká kvázigrupa pre $(x, y) \in T^*$.

Pre prvočíselné $q \leq 594\,423$ sme experimentálne overili, že taká kvázigrupa existuje práve vtedy, keď $q \geq 13$ a zároveň $q \notin \{17, 29, 53\}$.

□

Pravdepodobnosť uvedenú v predchádzajúcom tvrdení sme ešte dodatočne experimentálne overili výpočtom skutočnej veľkosti množiny T^*, pre všetky prvočísla $q \equiv 1 \bmod 4$ a $q < 100\,000$, za danej dodatočnej podmienky. Použili sme na to Algoritmus 6, ktorý je uvedený v Kapitole 5. Výsledok tohto overenia je uvedený v grafe na Obrázku B.5 v prílohe tejto práce. Experimentálne overenie zrejme naznačuje správnosť našich výpočtov.

Na experimentálne overenie existencie maximálne neasociatívnej kvázigrupy na záver dôkazu Tvrdenia 3.6 sme využili Algoritmus 7, ktorý je tiež uvedený v Kapitole 5.

3.3.2 $q \equiv 3 \bmod 4$

V tejto sekcii je našim cieľom asymptotický odhad veľkosti množiny T^* za predpokladu $q \equiv 3 \bmod 4$, ktorý použijeme k určeniu pravdepodobnosti, s akou náhodne zvolená dvojica $(x, y) \in S'$ padne do T.

Podobne ako vo všetkých skúmaných prípadoch v tejto práci, aj v tomto prípade vychádzame pri asymptotickom odhade veľkosti množiny T^* z podmienok na náležanie dvojice $(x, y) \in S'$ do jednej z množín S_{ij}^{rs}, ktoré sú pre tento konkrétny prípad uvedené v Lemma 3.4.

Okrem podmienok zo spomenutého Lemma musíme pre asymptotické odhady doplniť podmienky z definície množiny S, ktoré vzhľadom na použitie transformácie danej vzťahom (3.1) vyžadujú, aby d aj $h = d^2 - d + 1$ boli štvorce, čo sa dá zapísať ako $\chi(d) = \chi(d^2 - d + 1) = 1$. Tieto podmienky pridáme až na záver našich úvah a teraz sa sústredíme na podmienky z Lemma 3.2, pomocou ktorých popíšeme množinu T^*.

Označme si polynómy, ktoré sa v jednotlivých podmienkach vyskytujú, takto

$$\begin{aligned}
&p_1(d) = d - 1, && p_2(d) = 2d^2 - 2d + 1,\\
&p_3(d) = 2d - 1, && p_4(d) = -d^3 + 2d^2 - 3d + 1,\\
&p_5(d) = -d^3 + d^2 - 2d + 1, && p_6(d) = d^2 - 2d + 2,\\
&p_7(d) = d^3 - 2d^2 + d - 1, && p_8(d) = d + 1,\\
&p_9(d) = d \qquad \text{a} && p_{10}(d) = d^2 - d + 1.
\end{aligned}$$

Tieto polynómy majú najviac 19 rôznych koreňov. Nás ale zaujíma asymptotický odhad, preto týchto niekoľko málo hodnôt d môžeme zanedbať a ďalej budeme predpokladať, že d nie je koreňom žiadneho z týchto polynómov.

Pre $e \in \{1, \ldots, 8\}$ a polynóm $p_e(d)$ definujeme množiny A_e a B_e vzťahom (3.2) a pre $e \in \{9, 10\}$ týmto vzťahom definujeme A_e. Keďže predpokladáme, že d nie je koreňom žiadneho z polynómov $p_e(d)$, zrejme platí $\overline{A_e} = B_e$.

Budeme postupovať ako v obecnom prípade uvedenom v sekcii 1.4 na strane 13 a vyjadríme množinu T^* pomocou množín A_e a B_e. Preto potrebujeme pomocou množín A_e a B_e zapísať najprv množiny S_{ij}^{rs} a $\overline{S_{ij}^{rs}}$. Platí

$$\begin{aligned}
S_{01}^{10} =& B_1,\\
S_{10}^{00} =& A_1 \cap A_2,\\
S_{01}^{11} =& A_1 \cap A_3,\\
S_{00}^{01} =& A_1 \cap A_4 \cap A_5,\\
S_{10}^{10} =& ((B_6 \cap A_7) \cup (A_6 \cap B_7)) \cap ((B_6 \cap A_2) \cup (A_6 \cap B_2)) \cap\\
& ((A_6 \cap A_8 \cap A_1) \cup (A_6 \cap B_8 \cap B_1) \cup (B_6 \cap B_8 \cap A_1) \cup (B_6 \cap A_8 \cap B_1)).
\end{aligned}$$

$$\begin{aligned}
\overline{S_{01}^{10}} =& A_1,\\
\overline{S_{10}^{00}} =& B_1 \cup B_2,\\
\overline{S_{01}^{11}} =& B_1 \cup B_3,\\
\overline{S_{00}^{01}} =& B_1 \cup B_4 \cup B_5,\\
\overline{S_{10}^{10}} =& ((A_6 \cup B_7) \cap (B_6 \cup A_7)) \cup ((A_6 \cup B_2) \cap (B_6 \cup A_2)) \cup\\
& ((B_6 \cup B_8 \cup B_1) \cap (B_6 \cup A_8 \cup A_1) \cap (A_6 \cup A_8 \cup B_1) \cap (A_6 \cup B_8 \cup A_1)).
\end{aligned}$$

Ako je uvedené v (1.13), je množina T^* prienikom týchto množín $\overline{S_{ij}^{rs}}$. Platí

$$\begin{aligned}
T^* =& A_1 \cap (B_1 \cup B_2) \cap (B_1 \cup B_3) \cap (B_1 \cup B_4 \cup B_5) \cap\\
& (((A_6 \cup B_7) \cap (B_6 \cup A_7)) \cup ((A_6 \cup B_2) \cap (B_6 \cup A_2)) \cup\\
& ((B_6 \cup B_8 \cup B_1) \cap (B_6 \cup A_8 \cup A_1) \cap (A_6 \cup A_8 \cup B_1) \cap (A_6 \cup B_8 \cup A_1))).
\end{aligned}$$

Množinu T^* však potrebujeme zapísať ako zjednotenie disjunktných množín. Pri úprave výrazu využijeme skutočnosť, že pre množiny A a B platí

$$(A \cup \overline{B}) \cap (\overline{A} \cup B) = (A \cap B) \cup (\overline{A} \cap \overline{B}). \tag{3.6}$$

Potom zrejme platí

$$\begin{aligned}T^* =& A_1 \cap B_2 \cap B_3 \cap (B_4 \cup B_5) \cap ((A_6 \cap A_7) \cup (B_6 \cap B_7) \cup B_6 \cup \\ & ((B_6 \cup A_8 \cup A_1) \cap (A_6 \cup B_8 \cup A_1))), \\ =& A_1 \cap B_2 \cap B_3 \cap (B_4 \cup B_5) \cap ((A_6 \cap A_7) \cup B_6 \cup ((B_6 \cup A_8) \cap (A_6 \cup B_8))), \\ =& A_1 \cap B_2 \cap B_3 \cap (B_4 \cup B_5) \cap ((A_6 \cap A_7) \cup B_6 \cup (B_6 \cap B_8) \cup (A_6 \cap A_8)), \\ =& A_1 \cap B_2 \cap B_3 \cap (B_4 \cup B_5) \cap ((A_6 \cap (A_7 \cup A_8)) \cup B_6).\end{aligned}$$

A ďalej využijeme, že vzťah

$$A \cup B = (\overline{A} \cap B) \cup (A \cap \overline{B}) \cup (A \cap B) \tag{3.7}$$

je vyjadrenie zjednotenia množín A a B pomocou zjednotenia disjunktných množín. Vďaka tomu vidíme, že množinu $(B_4 \cup B_5)$ vieme zapísať ako zjednotenie 3 disjunktných množín, kde každú z týchto 3 množín definujú 2 polynómy.

Výraz $(A_6 \cap (A_7 \cup A_8)) \cup B_6$ je už zrejme zjednotenie disjunktných množín $A_6 \cap (A_7 \cup A_8)$ a B_6. Pre množinu $A_6 \cap (A_7 \cup A_8)$ nám ostáva aplikovať vzťah (3.7) na $A_7 \cup A_8$, čo znamená, že túto množinu zapíšeme ako zjednotenie 3 disjunktných množín daných 3 polynómami.

Celkovo teda dostávame, že množinu T^* môžeme zapísať ako zjednotenie $3 + 3 \cdot 3 = 12$ disjunktných množín, kde pre každú z týchto množín musíme kvôli asymptotickým odhadom pridať ešte podmienku $\chi(d) = \chi(d^2 - d + 1) = 1$ čo je ekvivalentné tomu, že do prieniku množín u každej z 12 disjunktných množín pridáme množiny A_9 a A_{10}. Preto sú 3 disjunktné množiny dané 8 polynómami $p_1(d)$, $p_2(d)$, $p_3(d)$, $p_4(d)$, $p_5(d)$, $p_6(d)$, $p_9(d)$ a $p_{10}(d)$ so súčtom stupňov 15. Zvyšných 9 disjunktných množín je daných všetkými 10 polynómami $p_e(d)$ so súčtom stupňov 19. Zoznam všetkých disjunktných množín je uvedený v Tabuľke A.6, ktorá sa nachádza v prílohe tejto práce.

Sme pripravení pristúpiť k samotnému asymptotického odhadu veľkosti T^*, ktorý uvedieme v nasledujúcom tvrdení.

Tvrdenie 3.7. *Predpokladajme $q \equiv 3 \bmod 4$, $q > 5$. Pre náhodne zvolené $(a, b) \in \Sigma$ také, že $(a, b) = \Psi^{-1}((x, y))$, kde x a y spĺňajú: $(x, y) \in S$ a $f_1(x, y) = 0$, je $Q_{a,b}$ maximálne neasociatívna kvázigrupa s pravdepodobnosťou $\approx 0{,}082$. Navyše platí, že maximálne neasociatívna kvázigrupa $Q_{a,b}$ spĺňajúca tieto podmienky vždy existuje pre $q > 499\,831$ a pre prvočíselné $q \leq 499\,831$ taká kvázigrupa existuje práve vtedy, keď $q \geq 23$ a zároveň $q \notin \{59, 67, 71\}$.*

Dôkaz. Dôkaz začneme odhadom asymptotickej veľkosti množiny T^*. Z diskusie pred týmto tvrdením plynie, že množinu T^* vieme zapísať ako zjednotenie 12 navzájom disjunktných množín. Preto Vetu 1.6 aplikujeme na každú z týchto množín samostatne a jednotlivé odhady sčítame.

Najprv overíme, že sú splnené predpoklady Vety 1.6. Polynómy, ktoré budeme vo vete využívať sú práve polynómy $p_1(d), \ldots, p_{10}(d)$. Z Lemma 4.3 plynie, že sa jedná o bezštvorcový zoznam polynómov, čím je predpoklad vety splnený.

V zozname týchto polynómov môže byť najviac 19 rôznych koreňov. Keďže nás zaujíma asymptotický odhad, môžeme týchto niekoľko hodnôt d zanedbať. Preto pridaním členu s hodnotou 19 do nášho odhadu môžeme predpokladať, že d nie je koreňom žiadneho z týchto polynómov.

Teraz už môžeme aplikovať Vetu 1.6 a dostávame

$$\left||T^*| - (9 \cdot 2^{-10} + 3 \cdot 2^{-8})q\right| < (\sqrt{q} + 1)108 + 19. \tag{3.8}$$

Z toho je vidno, že

$$\lim_{q \to \infty} \frac{|T^*|}{q} \doteq 0{,}0205.$$

Ako sme uviedli na začiatku sekcie 3.3, platí $\left|S'\right| \approx (q-1)/4$. V spojení s asymptotickým odhadom veľkosti množiny T^* je zrejmé, že hľadaná pravdepodobnosť je približne 0,082.

Využijeme vzťah (3.8) a dostávame, že maximálne neasociatívna kvázigrupa $Q_{a,b}$ existuje, ak platí

$$(9 \cdot 2^{-10} + 3 \cdot 2^{-8})q > (\sqrt{q} + 1)108 + 19.$$

To platí práve vtedy, keď $q > 27\,746\,149$. Aj v tomto prípade, sa dá táto hodnota znížiť tak, že ako podmnožinu T^* si vezmeme množinu $U = A_1 \cap B_2 \cap B_3 \cap B_4 \cap B_8 \cap A_9 \cap A_{10}$, ktorá je daná 7 polynómami so súčtom stupňov 11. Na zoznam tých polynómov aplikujeme Vetu 1.6 a dostávame, že pre $(x, y) \in U$ existuje maximálne neasociatívna kvázigrupa $Q_{a,b}$ práve vtedy, keď

$$2^{-7}q > (\sqrt{q} + 1)11/2 + 11,$$

čo platí práve vtedy, keď $q > 499\,831$. Zrejme teda platí, že pre $q > 499\,831$ taká kvázigrupa existuje pre $(x, y) \in T^*$.

Pre prvočíselné $q \leq 499\,831$ sme experimentálne overili, že taká kvázigrupa existuje práve vtedy, keď $q \geq 23$ a zároveň $q \notin \{59, 67, 71\}$.

□

Rovnako aj v tomto prípade sme pravdepodobnosť uvedenú v predchádzajúcom tvrdení dodatočne experimentálne overili výpočtom skutočnej veľkosti množiny T^*. V tomto prípade je výsledok tohto overenia uvedený v grafe, ktorý je uvedený na Obrázku B.6 v prílohe tejto práce. Experimentálne overenie zrejme naznačuje správnosť našich výpočtov.

Na experimentálne overenie existencie maximálne neasociatívnej kvázigrupy na záver dôkazu Tvrdenia 3.7 sme opäť využili Algoritmus 7.

4. $g_1(x, y) = 0$

Náš postup v prípade predpokladu $g_1(x, y) = 0$ bude podobný s tým, aký sme použili pri výpočtoch v prípade, ktorý využíval predpoklad $t_1(x, y) = 0$, keďže v tomto prípade môžeme položiť $y = 2x - x^2$. Opäť začneme tým, že Tvrdenie 1.26 a Tvrdenie 1.27 uvedieme v podobe, ktorá využíva uvedený dodatočný predpoklad a tieto tvrdenia následne využijeme k asymptotickým odhadom veľkosti množiny T^*.

4.1 Tvrdenie 1.26 pre prípad $g_1(x, y) = 0$

V tejto sekcii sa zameráme na Tvrdenie 1.26 a uvedieme podmienky pre množiny S_{ij}^{rs}, ktoré musí spĺňať $(x, y) \in S$, aby $(x, y) \in S_{ij}^{rs}$, a to za dodatočnej podmienky, že je daný vzťah medzi x a y taký, že pre polynóm $g_1(x, y) = x^2 + y - 2x$ platí $g_1(x, y) = 0$. Ako sme už uviedli, budeme predpokladať $y = 2x - x^2$. Pri tomto predpoklade budú polynómy uvedené v podmienkach iba v jednej neznámej x a na miesto dvojice $(x, y) \in S$ budeme písať $(x, 2x - x^2) \in S$.

Lemma 4.1. *Podmienky pre neprázdne množiny S_{ij}^{rs} uvedené v Tvrdení 1.26 majú v prípade dodatočnej podmienky $g_1(x, y) = 0$ tvar:*

$$
\begin{aligned}
&S_{11}^{00} = S_{11}^{01} = S_{00}^{10} = S_{01}^{01} = \emptyset,\\
&(x, 2x - x^2) \in S_{00}^{00} \iff \chi(x - 1) = 1,\\
&(x, 2x - x^2) \in S_{00}^{11} \iff \chi((x - 3)(x - 1)) = \chi(2x - 3) = -1,\\
&(x, 2x - x^2) \in S_{11}^{10} \iff \chi(x - 1) = -1 \text{ a } \chi(x^2 - x + 1) = \chi(x^2 - 2x + 2) = 1,\\
&(x, 2x - x^2) \in S_{00}^{01} \iff \chi(x - 1) = -1 \text{ a } \chi(x^2 - x - 1) = \chi(2x - 3) = 1,\\
&(x, 2x - x^2) \in S_{10}^{10} \iff \chi((x^2 - x + 1)(x^2 - 3x + 1)) = -1,\\
&\qquad\qquad\qquad\quad \chi((x^2 - x + 1)(x^2 - 3x + 3)) = -1 \text{ a}\\
&\qquad\qquad\qquad\quad \chi((x^2 - x + 1)(x - 1)) = \begin{cases} 1 & \text{ak } q \equiv 1 \bmod 8,\\ -1 & \text{ak } q \equiv 5 \bmod 8. \end{cases}
\end{aligned}
$$

Dôkaz. Tvrdenie 1.26 predpokladá $q \equiv 1 \bmod 4$, teda platí $\chi(-1) = 1$, a to budeme v celom dôkaze predpokladať. Ďalej toto tvrdenie uvádza $\varepsilon = \chi(x - y)$. Využitím predpokladu $y = 2x - x^2$ dostávame $\varepsilon = \chi(x - y) \overset{y=2x-x^2}{=} \chi((x - 1)x) = \chi(x - 1)$.

Do pôvodnej podoby tohto tvrdenia teda dosadíme $y = 2x - x^2$ a $\varepsilon = \chi(x - 1)$ a určíme, ako vyzerajú jednotlivé podmienky pre množiny S_{ij}^{rs} využitím predpokladu $\chi(-1) = 1$ a ďalších vlastností kvadratického charakteru χ.

Pri zápise jednotlivých podmienok využijeme symbol $\overset{?}{=}$ tak, že na ľavej strane tohto symbolu bude uvedená hodnota χ určitého polynómu v danej podmienke a na pravej strane symbolu $\overset{?}{=}$ bude výraz, ktorému sa musí výraz na ľavej strane rovnať, aby bola podmienka splnená.

Množina S_{11}^{00} je prázdna pretože je vidno, že podmienka $\chi(f_1(x, y)) \overset{y=2x-x^2}{=} \chi((x - 1)^3 x) = \chi(x - 1) \overset{?}{=} -\chi(x - 1)$ nemá riešenie, keďže predpokladáme $x \neq 1$.

Množiny S_{11}^{01} a S_{00}^{10} sú prázdne, pretože podmienka $\chi(1-x) = \chi(x-1) \stackrel{?}{=} -\chi(x-1)$ nemá riešenie.

V prípade S_{00}^{00} majú podmienky po dosadení za y a ε tvar

- $\chi(1-x) \stackrel{?}{=} \chi(x-1)$ (platí vždy z predpokladu $\chi(-1)=1$),
- $\chi(1-y) \stackrel{y=2x-x^2}{=} \chi((x-1)^2) = 1 \stackrel{?}{=} \chi(x-1)$.

V prípade S_{00}^{11} majú podmienky tvar

- $\chi(f_3(x,y)) \stackrel{y=2x-x^2}{=} \chi(x^2(x-3)(x-1)^2) = \chi(x-3) \stackrel{?}{=} -\chi(x-1)$, a to sa dá zapísať ako $\chi(x-3)\chi(x-1) = \chi((x-3)(x-1)) \stackrel{?}{=} -1$,
- $\chi(f_4(x,y)) \stackrel{y=2x-x^2}{=} \chi(-x^2(x-1)(2x-3)) = \chi((x-1)(2x-3)) \stackrel{?}{=} -\chi(x-1)$, a to sa dá zapísať ako $\chi((x-1)^2(2x-3)) = \chi(2x-3) \stackrel{?}{=} -1$.

V prípade S_{11}^{10} majú podmienky tvar

- $\chi(1-y) \stackrel{y=2x-x^2}{=} 1 \stackrel{?}{=} -\chi(x-1)$, teda $\chi(x-1) \stackrel{?}{=} -1$,
- $\chi(x+1-y) \stackrel{y=2x-x^2}{=} \chi(x^2-x+1) \stackrel{?}{=} 1$,
- $\chi(f_2(x,y)) \stackrel{y=2x-x^2}{=} \chi(x(x-1)(x^2-2x+2)) = \chi((x-1)(x^2-2x+2)) \stackrel{?}{=} \chi(x-1)$, a to môžeme zapísať ako $\chi((x-1)^2(x^2-2x+2)) = \chi(x^2-2x+2) \stackrel{?}{=} 1$.

V prípade S_{00}^{01} majú podmienky tvar

- Rovnako ako u S_{11}^{10}: $\chi(x-1) \stackrel{?}{=} -1$,
- $\chi(y+xy-x) \stackrel{y=2x-x^2}{=} \chi(-x(x^2-x-1)) = \chi(x^2-x-1) \stackrel{?}{=} 1$,
- Rovnako ako u S_{00}^{11} až na pravú stranu: $\chi(2x-3) \stackrel{?}{=} 1$.

V prípade S_{01}^{01} sa využíva $\eta = \chi(y+1-x) \stackrel{y=2x-x^2}{=} \chi(-x^2+x+1)$. Keďže predpokladáme $g_1(x,y)=0$, tak z podmienky $\chi(g_1(x,y)) \stackrel{?}{=} -\eta\varepsilon$ by po dosadení muselo platiť $0 \stackrel{?}{=} -\chi((-x^2+x+1)(x-1))$. Keďže by riešením boli len tie x, ktoré sú koreňom polynómu $-x^2+x+1$, a nás zajímajú len asymptotické odhady, môžeme tieto hodnoty x zanedbať a množinu S_{01}^{01} pri asymptotických odhadoch nebrať do úvahy, čo v znení tvrdenia zapíšeme ako prázdnu množinu.

V prípade S_{10}^{10} sa využíva $\eta = \chi(x+1-y) \stackrel{y=2x-x^2}{=} \chi(x^2-x+1)$ a potom $\eta\varepsilon = \chi((x^2-x+1)(x-1))$. Jednotlivé podmienky teda majú tvar

- $\chi(x+xy-y) \stackrel{y=2x-x^2}{=} \chi(-x(x^2-3x+1)) = \chi(x^2-3x+1) \stackrel{?}{=} -\chi(x^2-x+1)$, a to môžeme zapísať ako $\chi((x^2-3x+1)(x^2-x+1)) \stackrel{?}{=} -1$,
- $\chi(g_2(x,y)) \stackrel{y=2x-x^2}{=} \chi(x(x-1)(x^2-3x+3)) = \chi((x-1)(x^2-3x+3)) \stackrel{?}{=} -\chi((x^2-x+1)(x-1))$, a to môžeme zapísať ako $\chi((x-1)^2(x^2-3x+3)(x^2-x+1)) = \chi((x^2-3x+3)(x^2-x+1)) \stackrel{?}{=} -1$,

- $\chi(g_3(x,y)) \overset{y=2x-x^2}{=} \chi(2x(x-1)^2) = \chi(2) \overset{?}{=} \chi((x^2-x+1)(x-1))$. To musíme rozdeliť na 2 prípady v závislosti na hodnote $\chi(2)$ a to tak, že
$$\chi((x^2-x+1)(x-1)) = \begin{cases} 1 & \text{ak } q \equiv 1 \bmod 8, \\ -1 & \text{ak } q \equiv 5 \bmod 8. \end{cases}$$

Spojením všetkých uvedených podmienok pre množiny S_{ij}^{rs} a rozlíšením na 2 situácie v závislosti na q mod 8 dostávame dané lemma.

□

4.2 Tvrdenie 1.27 pre prípad $g_1(x, y) = 0$

V tejto sekcii sa zameráme na Tvrdenie 1.27 a rovnako ako v predchádzajúcej sekcii uvedieme podmienky pre množiny S_{ij}^{rs}, ktoré musí spĺňať $(x,y) \in S$, aby $(x,y) \in S_{ij}^{rs}$, a to za dodatočnej podmienky, že je daný vzťah medzi x a y taký, že pre polynóm $g_1(x,y) = x^2 + y - 2x$ platí $g_1(x,y) = 0$. Budeme teda predpokladať $y = 2x - x^2$.

Lemma 4.2. *Podmienky pre neprázdne množiny S_{ij}^{rs} uvedené v Tvrdení 1.27 majú v prípade dodatočnej podmienky $g_1(x,y) = 0$ tvar:*

$$\begin{aligned}
&S_{01}^{00} = S_{10}^{11} = S_{11}^{01} = S_{00}^{10} = S_{01}^{01} = \emptyset, \\
&(x, 2x-x^2) \in S_{01}^{10} \iff \chi(1-x) = -1, \\
&(x, 2x-x^2) \in S_{10}^{00} \iff \chi(1-x) = \chi(x^2-3x+3) = 1, \\
&(x, 2x-x^2) \in S_{01}^{11} \iff \chi(1-x) = 1 \ a \ \chi(x^2-x-1) = -1, \\
&(x, 2x-x^2) \in S_{11}^{10} \iff \chi(1-x) = \chi(-x^2+2x-2) = 1 \ a \ \chi(x^2-x+1) = -1, \\
&(x, 2x-x^2) \in S_{00}^{01} \iff \chi(1-x) = \chi(x^2-x-1) = \chi(2x-3) = 1, \\
&(x, 2x-x^2) \in S_{10}^{10} \iff \chi((x^2-x+1)(x^2-3x+1)) = -1, \\
&\qquad\qquad\qquad\quad \chi((x^2-x+1)(x^2-3x+3)) = -1 \ a \\
&\qquad\qquad\qquad\quad \chi((x^2-x+1)(1-x)) = \begin{cases} 1 & ak\ q \equiv 7 \bmod 8, \\ -1 & ak\ q \equiv 3 \bmod 8. \end{cases}
\end{aligned}$$

Dôkaz. V celom dôkaze budeme vychádzať z predpokladov Tvrdenia 1.27 a budeme predpokladať $q \equiv 3 \bmod 4$ a teda $\chi(-1) = -1$.

Do pôvodnej podoby tohto tvrdenia dosadíme $y = 2x - x^2$ a určíme, ako vyzerajú jednotlivé podmienky pre množiny S_{ij}^{rs} využitím predpokladu $\chi(-1) = -1$ a ďalších vlastností kvadratického charakteru χ.

Pri zápise jednotlivých podmienok využijeme symbol $\overset{?}{=}$ tak, že na ľavej strane tohto symbolu bude uvedená hodnota χ určitého polynómu v danej podmienke a na pravej strane symbolu $\overset{?}{=}$ bude hodnota, ktorú má výraz na ľavej strane nadobudnúť, aby podmienka platila.

Množiny S_{01}^{00}, S_{10}^{11}, S_{11}^{01} a S_{00}^{10} sú prázdne, pretože podmienka $\chi((1-x)(x-y)) \overset{y=2x-x^2}{=} \chi(-x(x-1)^2) = \chi(-1) \overset{?}{=} 1$ zrejme nie je splnená nikdy za predpokladu $\chi(-1) = -1$.

Množina S_{01}^{01} je prázdna, pretože podmienka $\chi(g_1(x,y)(y-x)(x-1-y)) = \chi(0) \overset{?}{=} 1$ nie je splnená nikdy.

V prípade S_{01}^{10} majú podmienky po dosadení za y tvar

- $\chi((1-y)(x-y)) \overset{y=2x-x^2}{=} \chi(x(x-1)^3) = \chi(x-1) \overset{?}{=} 1$,
- $\chi((1-x)(y-x)) \overset{y=2x-x^2}{=} \chi(x(x-1)^2) \overset{?}{=} 1$, táto podmienka je splnená vždy.

V prípade S_{10}^{00} majú podmienky tvar

- $\chi((1-y)(y-x)) \overset{y=2x-x^2}{=} \chi(-x(x-1)^3) = \chi(1-x) \overset{?}{=} 1$,
- $\chi(g_2(x,y)(x-y)) \overset{y=2x-x^2}{=} \chi(x^2(x-1)^2(x^2-3x+3)) = \chi(x^2-3x+3) \overset{?}{=} 1$.

V prípade S_{01}^{11} majú podmienky tvar

- Rovnako ako u S_{10}^{00}: $\chi(1-x) \overset{?}{=} 1$,
- $\chi(g_4(x,y)(y-x)) \overset{y=2x-x^2}{=} \chi(-x^2(x-1)^2(x^2-x-1)) = \chi(-x^2+x+1) \overset{?}{=} 1$.

V prípade S_{11}^{10} majú podmienky tvar

- Rovnako ako u S_{10}^{00}: $\chi(1-x) \overset{?}{=} 1$,
- $\chi(y-1-x) \overset{y=2x-x^2}{=} \chi(-x^2+x-1) \overset{?}{=} 1$,
- $\chi((y-x)f_2(x,y)) \overset{y=2x-x^2}{=} \chi(-(x-1)^2x^2(x^2-2x+2)) = \chi(-x^2+2x-2) \overset{?}{=} 1$.

V prípade S_{00}^{01} majú podmienky tvar

- Rovnako ako u S_{10}^{00}: $\chi(1-x) \overset{?}{=} 1$,
- $\chi(x-xy-y) \overset{y=2x-x^2}{=} \chi(x(x^2-x-1)) = \chi(x^2-x-1) \overset{?}{=} 1$,
- $\chi((y-x)f_4(x,y)) \overset{y=2x-x^2}{=} \chi(x^3(x-1)^2(2x-3)) = \chi(2x-3) \overset{?}{=} 1$.

V prípade S_{10}^{10} majú podmienky tvar

- $\chi((y-xy-x)(y-1-x)) \overset{y=2x-x^2}{=} \chi(-x(x^2-3x+1)(x^2-x+1)) = \chi(-(x^2-3x+1)(x^2-x+1)) \overset{?}{=} 1$,
- $\chi(g_2(x,y)(x-y)(y-1-x)) \overset{y=2x-x^2}{=} \chi(-x^2(x-1)^2(x^2-x+1)(x^2-3x+3)) = \chi(-(x^2-x+1)(x^2-3x+3)) \overset{?}{=} 1$,
- $\chi(g_3(x,y)(x-y)(y-1-x)) \overset{y=2x-x^2}{=} \chi(-2x^2(x-1)^3(x^2-x+1)) = \chi(2(1-x)(x^2-x+1)) \overset{?}{=} 1$.

Spojením všetkých uvedených podmienok pre množiny S_{ij}^{rs} a rozlíšením na 2 situácie v závislosti na q mod 8 dostávame dané lemma.

□

4.3 Asymptotické odhady

V tejto časti práce uvedieme asymptotický odhad veľkosti množiny T na základe popisu množiny T^* uvedeného v sekcii 1.4, a to za podmienky $g_1(x, y) = 0$. Tento asymptotický odhad následne využijeme pri určení pravdepodobnosti, s akou pri náhodnej voľbe $(x, 2x - x^2) \in S'$ padne dvojica $(x, 2x - x^2)$ do T. Pri dodatočnej podmienke $g_1(x, y) = 0$ je $S' = \{(x, y) \in S : y = 2x - x^2\}$.

Dôležitou informáciou pre realizáciu asymptotického odhadu sú podmienky pre množiny S_{ij}^{rs} získané v Lemma 4.1 a v Lemma 4.2, ktoré vychádzali z Tvrdenia 1.26 a z Tvrdenia 1.27 pridaním dodatočného predpokladu $g_1(x, y) = 0$. V oboch prípadoch sa podmienky založené na polynómoch v x a y transformovali na podmienky s polynómami v jednej neznámej x. Vďaka tomu môžeme aj v tomto prípade po dodatočných úvahách priamo aplikovať Vetu 1.6. Tieto podmienky sa v závislosti na q opäť delia na 4 skupiny

- $q \equiv 1 \bmod 8$,
- $q \equiv 5 \bmod 8$,
- $q \equiv 3 \bmod 8$,
- $q \equiv 7 \bmod 8$.

Pre každý z týchto prípadov musíme realizovať asymptotický odhad veľkosti množiny T samostatne. Postupne rozoberieme jednotlivé prípady vo zvyšku tejto kapitoly.

Pozrime sa na veľkosť množiny S'. Zaujíma nás teda počet $y \in \mathbb{F}_q$ tak, že x aj $2x - x^2$ sú nenulové štvorce. Využijeme, že platí $2x - x^2 = x(2 - x)$, a teda ak budeme predpokladať x štvorec, stačí sa nám pýtať, či je aj $2 - x$ štvorec. Využijeme Vetu 1.4, podľa ktorej to splňuje $\approx 1/4$ zo všetkých x. Keďže budeme pracovať s asymptotickými odhadmi, stačí nám približná veľkosť S', teda platí $\left|S'\right| \approx (q - 1)/4$.

Na odhad veľkosti množiny T budeme používať Vetu 1.6. Predpoklady tejto vety však vyžadujú, aby bol zoznam polynómov bezštvorcový. Preto si zhrnieme zoznam polynómov, ktoré budeme v uvedených 4 prípadoch v závislosti na q potrebovať a ukážeme, že je to naozaj bezštvorcový zoznam. V ďalšej časti sa už na toto lemma budeme len odkazovať.

Lemma 4.3. *Zoznam polynómov* x, $2 - x$, $x - 1$, $x - 3$, $2x - 3$, $x^2 - x + 1$, $x^2 - 2x + 2$, $x^2 - x - 1$, $x^2 - 3x + 1$ *a* $x^2 - 3x + 3$ *je bezštvorcový, ak platí* $\mathrm{char}(\mathbb{F}_q) > 5$.

Dôkaz. Je zrejmé, že lineárne polynómy majú navzájom rôzne korene v prípade, že $\mathrm{char}(\mathbb{F}_q) > 3$ a tiež žiaden z kvadratických polynómov s nimi koreň nezdieľa.

Kvadratické polynómy x^2-x+1, x^2-2x+2, x^2-x-1, x^2-3x+1 a x^2-3x+3 majú korene v tomto poradí $(1 \pm \sqrt{-3})/2$, $(2 \pm \sqrt{-4})/2$, $(1 \pm \sqrt{5})/2$, $(3 \pm \sqrt{5})/2$ a $(3 \pm \sqrt{-3})/2$. Z toho je vidno, že nezdieľajú koreň a pridaním predpokladu $\mathrm{char}(\mathbb{F}_q) > 5$ navyše nedôjde ani k tomu, aby nejaký polynóm mal dvojnásobný koreň.

Celkovo teda dostávame, že vynásobením ľubovoľných polynómov daného zoznamu nezískame štvorec a preto sa jedná o bezštvorcový zoznam polynómov.

□

4.3.1 $q \equiv 1 \bmod 8$

V tejto sekcii je našim cieľom asymptotický odhad veľkosti množiny T^* za predpokladu $q \equiv 1 \bmod 8$, ktorý použijeme k určeniu pravdepodobnosti, s akou náhodne zvolená dvojica $(x, 2x - x^2) \in S'$ padne do T.

Podobne ako vo všetkých skúmaných prípadoch v tejto práci vychádzame v tomto prípade pri asymptotickom odhade veľkosti množiny T^* z podmienok, ktoré musí spĺňať x, aby dvojica $(x, 2x - x^2) \in S'$ patrila do jednej z množín S_{ij}^{rs}. Pre situáciu v tejto časti práce sú tieto podmienky uvedené v Lemma 4.1.

Okrem podmienok zo spomenutého Lemma musíme pre asymptotické odhady doplniť podmienky z definície množiny S, ktoré vyžadujú, aby x aj $y = 2x - x^2 = x(2 - x)$ boli štvorce, čo sa dá zapísať ako $\chi(x) = \chi(2 - x) = 1$. Tieto podmienky pridáme až na záver našich úvah a teraz sa sústredíme na podmienky z Lemma 4.1, pomocou ktorých popíšeme množinu T^*.

Označme si polynómy, ktoré sa v jednotlivých podmienkach vyskytujú, takto

$$\begin{aligned} p_1(x) &= x - 1, & p_2(x) &= x - 3, \\ p_3(x) &= 2x - 3, & p_4(x) &= x^2 - x + 1, \\ p_5(x) &= x^2 - 2x + 2, & p_6(x) &= x^2 - x - 1, \\ p_7(x) &= x^2 - 3x + 1, & p_8(x) &= x^2 - 3x + 3, \\ p_9(x) &= x \quad \text{a} & p_{10}(x) &= 2 - x. \end{aligned}$$

Tieto polynómy majú najviac 15 rôznych koreňov. Nás ale zaujíma asymptotický odhad, preto týchto niekoľko málo hodnôt x môžeme zanedbať a ďalej budeme predpokladať, že x nie je koreňom žiadneho z týchto polynómov.

Využijeme Označenie 1.28, ktoré musíme predefinovať pre našu konkrétnu situáciu a to tak, že $\langle p(x), \omega \rangle = \{(x, 2x - x^2) \in S' : \chi(p(x)) = \omega\}$, pre $p(x) \in \mathbb{F}_q[x]$ a $\omega \in \{1, -1\}$. To využijeme tak, že pre $e \in \{1, \ldots, 8\}$ a polynóm $p_e(x)$ položíme

$$A_e = \langle p_e(x), 1 \rangle \qquad \text{a} \qquad B_e = \langle p_e(x), -1 \rangle. \tag{4.1}$$

V prípade $e \in \{9, 10\}$ definujeme týmto spôsobom A_e.

Keďže predpokladáme, že x nie je koreňom žiadneho z polynómov $p_e(x)$, zrejme platí $\overline{A_e} = B_e$, čo budeme využívať.

Budeme postupovať ako v obecnom prípade uvedenom v sekcii 1.4 na strane 13 a vyjadríme množinu T^* pomocou množín A_e a B_e. Preto potrebujeme pomocou množín A_e a B_e zapísať najprv množiny S_{ij}^{rs} a $\overline{S_{ij}^{rs}}$. Platí

$$\begin{aligned} S_{00}^{00} &= A_1, \\ S_{00}^{11} &= ((B_1 \cap A_2) \cup (A_1 \cap B_2)) \cap B_3, \\ S_{11}^{10} &= B_1 \cap A_4 \cap A_5, \\ S_{00}^{01} &= B_1 \cap A_6 \cap A_3, \\ S_{10}^{10} &= ((B_4 \cap A_7) \cup (A_4 \cap B_7)) \cap \\ &\quad ((B_4 \cap A_8) \cup (A_4 \cap B_8)) \cap \\ &\quad ((A_4 \cap A_1) \cup (B_4 \cap B_1)). \end{aligned}$$

$$
\begin{aligned}
\overline{S_{00}^{00}} =& B_1,\\
\overline{S_{00}^{11}} =& ((A_1 \cup B_2) \cap (B_1 \cup A_2)) \cup A_3,\\
\overline{S_{11}^{10}} =& A_1 \cup B_4 \cup B_5,\\
\overline{S_{00}^{01}} =& A_1 \cup B_6 \cup B_3,\\
\overline{S_{10}^{10}} =& ((A_4 \cup B_7) \cap (B_4 \cup A_7)) \cup\\
& ((A_4 \cup B_8) \cap (B_4 \cup A_8)) \cup\\
& ((B_4 \cup B_1) \cap (A_4 \cup A_1)).
\end{aligned}
$$

Ako je uvedené v (1.13), je množina T^* prienikom týchto množín $\overline{S_{ij}^{rs}}$. Platí

$$
\begin{aligned}
T^* =& B_1 \cap (((A_1 \cup B_2) \cap (B_1 \cup A_2)) \cup A_3) \cap (A_1 \cup B_4 \cup B_5) \cap\\
& (A_1 \cup B_6 \cup B_3) \cap (((A_4 \cup B_7) \cap (B_4 \cup A_7)) \cup\\
& ((A_4 \cup B_8) \cap (B_4 \cup A_8)) \cup ((B_4 \cup B_1) \cap (A_4 \cup A_1))).
\end{aligned}
$$

Množinu T^* však potrebujeme zapísať ako zjednotenie disjunktných množín. Pri úprave výrazu využijeme skutočnosť, že pre množiny A a B platí

$$
(A \cup \overline{B}) \cap (\overline{A} \cup B) = (A \cap B) \cup (\overline{A} \cap \overline{B}). \tag{4.2}
$$

Potom zrejme platí

$$
\begin{aligned}
T^* =& B_1 \cap ((A_1 \cap A_2) \cup (B_1 \cap B_2) \cup A_3) \cap (B_4 \cup B_5) \cap (B_6 \cup B_3) \cap\\
& ((A_4 \cap A_7) \cup (B_4 \cap B_7) \cup (A_4 \cap A_8) \cup (B_4 \cap B_8) \cup (B_4 \cap A_1) \cup (A_4 \cap B_1))\\
=& B_1 \cap ((B_1 \cap B_2) \cup A_3) \cap (B_4 \cup B_5) \cap (B_6 \cup B_3) \cap\\
& ((A_4 \cap A_7) \cup (B_4 \cap B_7) \cup (A_4 \cap A_8) \cup (B_4 \cap B_8) \cup A_4)\\
=& B_1 \cap (B_2 \cup A_3) \cap (B_6 \cup B_3) \cap (B_4 \cup B_5) \cap (A_4 \cup (B_4 \cap (B_7 \cup B_8))).
\end{aligned}
$$

A ďalej využijeme, že vzťah

$$
A \cup B = (\overline{A} \cap B) \cup (A \cap \overline{B}) \cup (A \cap B) \tag{4.3}
$$

je vyjadrenie zjednotenia množín A a B pomocou zjednotenia disjunktných množín. Potom je vidno, že pre $(B_2 \cup A_3) \cap (B_6 \cup B_3)$ platí

$$
\begin{aligned}
(B_2 \cup A_3) \cap (B_6 \cup B_3) =& (B_2 \cap B_3 \cap B_6) \cup (A_2 \cap A_3 \cap B_6) \cup\\
& (B_2 \cap A_3 \cap B_6) \cup (B_2 \cap B_3 \cap A_6),
\end{aligned}
$$

kde 4 množiny na pravej strane sú navzájom disjunktné a každá je daná 3 polynómami.

Ostáva nám zapísať ako zjednotenie disjunktných množín výraz $(B_4 \cup B_5) \cap (A_4 \cup (B_4 \cap (B_7 \cup B_8)))$.

Najprv teda platí $B_4 \cup B_5 = (B_4 \cap A_5) \cup (A_4 \cap B_5) \cup (B_4 \cap B_5)$. Vďaka tomu dostávame

$$
\begin{aligned}
(B_4 \cup B_5) \cap (A_4 \cup (B_4 \cap (B_7 \cup B_8))) =& (B_4 \cap A_5 \cap (B_7 \cup B_8)) \cup (A_4 \cap B_5) \cup\\
& (B_4 \cap B_5 \cap (B_7 \cup B_8)).
\end{aligned}
$$

V poslednom uvedenom výraze stačí nahradiť $B_7 \cup B_8$ podľa vzťahu (4.3), teda vo výsledku zapíšeme výraz $(B_4 \cup B_5) \cap (A_4 \cup (B_4 \cap (B_7 \cup B_8)))$ ako zjednotenie 7 disjunktných množín, kde 6 z týchto množín je daných 4 polynómami $p_4(x), p_5(x), p_7(x)$ a $p_8(x)$, a množina $A_4 \cap B_5$ je daná iba 2 polynómami $p_4(x)$ a $p_5(x)$.

Celkovo teda dostávame, že množinu T^* môžeme zapísať ako zjednotenie $4 \cdot 7 = 28$ disjunktných množín, kde pre každú z týchto množín musíme kvôli asymptotickým odhadom pridať ešte podmienku $\chi(x) = \chi(2 - x) = 1$ čo je ekvivalentné tomu, že do prieniku množín u každej z 28 disjunktných množín pridáme množiny A_9 a A_{10}. Preto 24 z týchto disjunktných množín je daných 10 polynómami $p_1(x), \ldots, p_{10}(x)$ so súčtom stupňov 15 a zvyšné 4 disjunktné množíny sú dané 8 polynómami $p_1(x), p_2(x), p_3(x), p_4(x), p_5(x), p_6(x), p_9(x), p_{10}(x)$ so súčtom stupňov 11, čo nám k asymptotickým odhadom stačí a nie je dôležité, aká má byť presne hodnota χ pre daný polynóm. Zoznam všetkých disjunktných množín je uvedený v Tabuľke A.7, ktorá sa nachádza v prílohe tejto práce.

Konečne sme pripravení pristúpiť k samotnému asymptotického odhadu veľkosti T^*, ktorý uvedieme v nasledujúcom tvrdení.

Tvrdenie 4.4. *Predpokladajme $q \equiv 1 \bmod 8$, $q > 5$. Pre náhodne zvolené $(a, b) \in \Sigma$ také, že $(a, b) = \Psi^{-1}((x, y))$, kde x a y spĺňajú: $(x, y) \in S$ a $g_1(x, y) = 0$, je $Q_{a,b}$ maximálne neasociatívna kvázigrupa s pravdepodobnosťou $\approx 0{,}156$. Navyše platí, že maximálne neasociatívna kvázigrupa $Q_{a,b}$ spĺňajúca tieto podmienky vždy existuje pre $q > 335\,223$ a pre prvočíselné $q \leq 335\,223$ taká kvázigrupa existuje práve vtedy, keď $q \geq 17$.*

Dôkaz. Dôkaz začneme odhadom asymptotickej veľkosti množiny T^*. Z diskusie pred týmto tvrdením plynie, že množinu T^* vieme zapísať ako zjednotenie 28 navzájom disjunktných množín. Preto Vetu 1.6 aplikujeme na každú z týchto množín samostatne a jednotlivé odhady sčítame.

Najprv overíme, že sú splnené predpoklady Vety 1.6. Polynómy, ktoré budeme vo vete využívať sú práve polynómy $p_1(x), \ldots, p_{10}(x)$. Z Lemma 4.3 plynie, že sa jedná o bezštvorcový zoznam polynómov, čím je predpoklad vety splnený.

V zozname týchto polynómov môže byť maximálne 15 rôznych koreňov. Keďže nás zaujíma asymptotický odhad, môžeme týchto niekoľko hodnôt x zanedbať. Preto pridaním členu s hodnotou 15 do nášho odhadu môžeme predpokladať, že x nie je koreňom žiadneho z týchto polynómov.

Teraz už môžeme aplikovať Vetu 1.6 a dostávame

$$\begin{aligned} \left||T^*| - (24 \cdot 2^{-10} + 4 \cdot 2^{-8})q\right| &< (\sqrt{q} + 1)(24 \cdot 15 + 4 \cdot 11)/2 + 15, \\ \left||T^*| - (24 \cdot 2^{-10} + 4 \cdot 2^{-8})q\right| &< (\sqrt{q} + 1)202 + 15. \end{aligned} \tag{4.4}$$

Z toho je vidno, že

$$\lim_{q \to \infty} \frac{|T^*|}{q} \doteq 0{,}0391.$$

Ako sme uviedli na začiatku sekcie 4.3, platí $\left|S'\right| \approx (q - 1)/4$. V spojení s asymptotickým odhadom veľkosti množiny T^* je zrejmé, že pri náhodnej voľbe x, ktoré spĺňuje $(x, 2x - x^2) \in S'$, padne dvojica $(x, 2x - x^2)$ do T^* s pravdepodobnosťou približne 0,156, čo je presne hľadaná pravdepodobnosť.

Využijeme vzťah (4.4) a dostávame, že maximálne neasociatívna kvázigrupa $Q_{a,b}$ existuje, ak platí

$$(24 \cdot 2^{-10} + 4 \cdot 2^{-8})q > (\sqrt{q} + 1)202 + 15.$$

To platí práve vtedy, keď $q > 26\,752\,418$. Aby sme túto hodnotu znížili, môžeme tento dôkaz existencie urobiť pre nejakú podmnožinu T^*, ktorá je popísaná menším počtom podmienok. Za takú podmnožinu T^* môžeme zvoliť množinu $B_1 \cap B_2 \cap B_3 \cap A_4 \cap B_5 \cap A_9 \cap A_{10}$, ktorú označme U. Ide o množinu danú 7 polynómami so súčtom stupňov 9. Na zoznam tých 7 polynómov, ktoré nám dávajú U, aplikujeme Vetu 1.6 a urobíme rovnaký trik ako pri dôkaze existencie pre celé T^*. Dostávame, že pre $(x, y) \in U$ existuje maximálne neasociatívna kvázigrupa $Q_{a,b}$ práve vtedy, keď

$$2^{-7}q > (\sqrt{q} + 1)9/2 + 9,$$

čo platí práve vtedy, keď $q > 335\,223$. Zrejme teda platí, že pre $q > 335\,223$ existuje taká kvázigrupa pre $(x, y) \in T^*$.

Pre prvočíselné $q \leq 335\,223$ sme experimentálne overili, že taká kvázigrupa existuje práve vtedy, keď $q \geq 17$.

□

Pravdepodobnosť uvedenú v predchádzajúcom tvrdení sme ešte dodatočne experimentálne overili výpočtom skutočnej veľkosti množiny T^*, pre všetky prvočísla $q \equiv 1 \bmod 8$ a $q < 100\,000$, za danej dodatočnej podmienky. Použili sme na to Algoritmus 6, ktorý je uvedený v Kapitole 5. Výsledok tohto overenia je uvedený v grafe na Obrázku B.7 v prílohe tejto práce. Experimentálne overenie zrejme naznačuje správnosť našich výpočtov.

Na experimentálne overenie existencie maximálne neasociatívnej kvázigrupy na záver dôkazu Tvrdenia 4.4 sme využili Algoritmus 7, ktorý je tiež uvedený v Kapitole 5.

4.3.2 $q \equiv 5 \bmod 8$

Tentokrát budeme predpokladať $q \equiv 5 \bmod 8$. Tento prípad je takmer identický s prípadom $q \equiv 1 \bmod 8$ v sekcii 4.3.1, od ktorého sa líši len v podmienke pre množinu S_{10}^{10} ako je vidno v Lemma 4.1. Nebudeme preto tomuto prípadu venovať veľa pozornosti, ale uvedieme len dôležité informácie k určeniu hľadanej pravdepodobnosti.

V tomto prípade teda využívame rovnaké polynómy ako v sekcii 4.3.1 a preto aj množiny A_e a B_e budú totožné s predchádzajúcim prípadom. Podmienky pre množiny S_{ij}^{rs} tvar teda tvar

$$\begin{aligned}
S_{00}^{00} =& A_1, \\
S_{00}^{11} =& ((B_1 \cap A_2) \cup (A_1 \cap B_2)) \cap B_3, \\
S_{11}^{10} =& B_1 \cap A_4 \cap A_5, \\
S_{00}^{01} =& B_1 \cap A_6 \cap A_3, \\
S_{10}^{10} =& ((B_4 \cap A_7) \cup (A_4 \cap B_7)) \cap \\
& ((B_4 \cap A_8) \cup (A_4 \cap B_8)) \cap \\
& ((B_4 \cap A_1) \cup (A_4 \cap B_1)).
\end{aligned}$$

Ďalej opäť postupujeme ako v obecnom prípade uvedenom v sekcii 1.4. Keďže je ďalší postup takmer identický s postupom v sekcii 4.3.1 uvedieme len zápis množiny T^* pomocou množín A_e a B_e, a potom transformáciu tohto zápisu na zjednotenie disjunktných množín. Platí teda

$$T^* = B_1 \cap (B_2 \cup A_3) \cap (B_6 \cup B_3) \cap (B_4 \cup B_5) \cap (B_4 \cup (A_4 \cap (A_7 \cup A_8))).$$

Opäť využijeme vzťah

$$\begin{aligned}(B_2 \cup A_3) \cap (B_6 \cup B_3) = &(B_2 \cap B_3 \cap B_6) \cup (A_2 \cap A_3 \cap B_6) \cup \\ &(B_2 \cap A_3 \cap B_6) \cup (B_2 \cap B_3 \cap A_6).\end{aligned}$$

A v tomto prípade ešte platí

$$\begin{aligned}(B_4 \cup B_5) \cap (B_4 \cup (A_4 \cap (A_7 \cup A_8))) = &(B_4 \cap A_5) \cup (B_4 \cap B_5) \cup \\ &(A_4 \cap B_5 \cap (A_7 \cup A_8)).\end{aligned}$$

V poslednom uvedenom výraze stačí nahradiť $A_7 \cup A_8$ podľa vzťahu (4.3). Vo výsledku zapíšeme výraz $(B_4 \cup B_5) \cap (B_4 \cup (A_4 \cap (A_7 \cup A_8)))$ ako zjednotenie 5 disjunktných množín, kde 3 z týchto množín sú dané 4 polynómami $p_4(x), p_5(x), p_7(x)$ a $p_8(x)$, a množiny $B_4 \cap A_5$ a $B_4 \cap B_5$ sú dané iba polynómami $p_4(x)$ a $p_5(x)$.

Celkovo teda môžeme množinu T^* zapísať ako zjednotenie $4 \cdot 5 = 20$ disjunktných množín, kde pre každú z týchto množín pridáme ešte prienik s A_9 a A_{10}. Preto 12 z týchto disjunktných množín je daných 10 polynómami $p_1(x), \ldots, p_{10}(x)$ so súčtom stupňov 15 a zvyšných 8 disjunktných množín je daných 8 polynómami $p_1(x), p_2(x), p_3(x), p_4(x), p_5(x), p_6(x), p_9(x), p_{10}(x)$ so súčtom stupňov 11, čo nám k asymptotickým odhadom stačí. Zoznam všetkých disjunktných množín je uvedený v Tabuľke A.8, ktorá sa nachádza v prílohe tejto práce.

Môžeme pristúpiť k asymptotického odhadu veľkosti T^*, ktorý uvedieme v nasledujúcom tvrdení.

Tvrdenie 4.5. *Predpokladajme $q \equiv 5 \bmod 8$. Pre náhodne zvolené $(a, b) \in \Sigma$ také, že $(a, b) = \Psi^{-1}((x, y))$, kde x a y spĺňajú: $(x, y) \in S$ a $g_1(x, y) = 0$, je $Q_{a,b}$ maximálne neasociatívna kvázigrupa s pravdepodobnosťou $\approx 0{,}172$. Navyše platí, že maximálne neasociatívna kvázigrupa $Q_{a,b}$ spĺňajúca tieto podmienky vždy existuje pre $q > 51\,511$ a pre prvočíselné $q \leq 51\,511$ taká kvázigrupa existuje práve vtedy, keď $q \geq 13$ a zároveň $q \neq 29$.*

Dôkaz. Dôkaz začneme odhadom asymptotickej veľkosti množiny T^*. Z diskusie pred týmto tvrdením plynie, že množinu T^* vieme zapísať ako zjednotenie 20 navzájom disjunktných množín. Preto Vetu 1.6 aplikujeme na každú z týchto množín samostatne a jednotlivé odhady sčítame.

Najprv overíme, že sú splnené predpoklady Vety 1.6. Polynómy, ktoré budeme vo vete využívať sú práve polynómy $p_1(x), \ldots, p_{10}(x)$. Z Lemma 4.3 plynie, že sa jedná o bezštvorcový zoznam polynómov, čím je predpoklad vety splnený.

V zozname týchto polynómov môže byť maximálne 15 rôznych koreňov. Keďže nás zaujíma asymptotický odhad, môžeme týchto niekoľko hodnôt x zanedbať. Preto pridaním členu s hodnotou 15 do nášho odhadu môžeme ďalej predpokladať, že x nie je koreňom žiadneho z týchto polynómov.

Teraz už môžeme aplikovať Vetu 1.6 a dostávame

$$\begin{aligned}\left||T^*| - (12 \cdot 2^{-10} + 8 \cdot 2^{-8})q\right| &< (\sqrt{q}+1)(12 \cdot 15 + 8 \cdot 11)/2 + 15,\\ \left||T^*| - (12 \cdot 2^{-10} + 8 \cdot 2^{-8})q\right| &< (\sqrt{q}+1)134 + 15. \end{aligned} \tag{4.5}$$

Z toho je vidno, že

$$\lim_{q\to\infty} \frac{|T^*|}{q} \doteq 0{,}043.$$

Opäť $\left|S'\right| \approx (q-1)/4$. V spojení s asymptotickým odhadom veľkosti množiny T^* je hľadaná pravdepodobnosť približne 0,172.

Využijeme vzťah (4.5) a dostávame, že maximálne neasociatívna kvázigrupa $Q_{a,b}$ existuje, ak platí

$$(12 \cdot 2^{-10} + 8 \cdot 2^{-8})q > (\sqrt{q}+1)134 + 15.$$

To platí práve vtedy, keď $q > 9\,732\,259$. Aj v tomto prípade, sa dá táto hodnota znížiť tak, že ako podmnožinu T^* si vezmeme množinu $U = B_1 \cap B_2 \cap B_3 \cap B_4 \cap A_9 \cap A_{10}$, ktorá je daná 6 polynómami so súčtom stupňov 7. Na zoznam tých polynómov aplikujeme Vetu 1.6 a dostávame, že pre $(x, y) \in U$ existuje maximálne neasociatívna kvázigrupa $Q_{a,b}$ práve vtedy, keď

$$2^{-6}q > (\sqrt{q}+1)7/2 + 7,$$

čo platí práve vtedy, keď $q > 51\,511$. Zrejme teda platí, že pre $q > 51\,511$ taká kvázigrupa existuje pre $(x, y) \in T^*$.

Pre prvočíselné $q \leq 51\,511$ sme experimentálne overili, že taká kvázigrupa existuje práve vtedy, keď $q \geq 13$ a zároveň $q \neq 29$.

□

Rovnako aj v tomto prípade sme pravdepodobnosť uvedenú v predchádzajúcom tvrdení dodatočne experimentálne overili výpočtom skutočnej veľkosti množiny T^*. V tomto prípade je výsledok tohto overenia uvedený v grafe, ktorý je uvedený na Obrázku B.8 v prílohe tejto práce. Experimentálne overenie zrejme naznačuje správnosť našich výpočtov.

Na experimentálne overenie existencie maximálne neasociatívnej kvázigrupy na záver dôkazu Tvrdenia 4.5 sme opäť využili Algoritmus 7.

4.3.3 $q \equiv 3 \bmod 8$

V tejto sekcii je našim cieľom asymptotický odhad veľkosti množiny T^* za predpokladu $q \equiv 3 \bmod 8$, ktorý využijeme k určeniu pravdepodobnosti, s akou náhodne zvolená dvojica $(x, 2x - x^2) \in S'$ padne do T^*.

Podobne ako vo všetkých skúmaných prípadoch v tejto práci vychádzame aj v tomto prípade pri asymptotickom odhade veľkosti množiny T^* z podmienok, ktoré musí spĺňať x, aby dvojica $(x, 2x - x^2) \in S'$ patrila do jednej z množín S_{ij}^{rs}. Pre situáciu v tejto časti práce sú tieto podmienky uvedené v Lemma 4.2.

Na záver našich úvah opäť nesmieme zabudnúť pridať požiadavku, aby platilo $\chi(x) = \chi(2 - x) = 1$. Teraz sa sústredíme na podmienky z Lemma 4.2, pomocou ktorých popíšeme množinu T^*.

Označme si polynómy, ktoré sa v jednotlivých podmienkach vyskytujú, takto

$$\begin{aligned}
&p_1(x) = 1 - x, && p_2(x) = x^2 - 3x + 3,\\
&p_3(x) = x^2 - x - 1, && p_4(x) = -x^2 + 2x - 2,\\
&p_5(x) = x^2 - x + 1, && p_6(x) = 2x - 3,\\
&p_7(x) = x^2 - 3x + 1, && p_8(x) = x \text{ a}\\
&p_9(x) = 2 - x.
\end{aligned}$$

Tieto polynómy majú najviac 14 rôznych koreňov. Nás ale zaujíma asymptotický odhad, preto týchto niekoľko málo hodnôt x môžeme zanedbať. Ďalej budeme predpokladať, že x nie je koreňom žiadneho z týchto polynómov.

Pre $e \in \{1, \ldots, 7\}$ a polynóm $p_e(x)$ definujeme množiny A_e a B_e vzťahom (4.1) a pre $e \in \{8, 9\}$ týmto vzťahom definujeme A_e. Keďže predpokladáme, že x nie je koreňom žiadneho z polynómov $p_e(x)$, zrejme platí $\overline{A_e} = B_e$.

Budeme postupovať ako v obecnom prípade uvedenom v sekcii 1.4 na strane 13 a vyjadríme množinu T^* pomocou množín A_e a B_e. Preto potrebujeme pomocou množín A_e a B_e zapísať najprv množiny S_{ij}^{rs} a $\overline{S_{ij}^{rs}}$. Platí

$$\begin{aligned}
S_{01}^{10} =& B_1,\\
S_{10}^{00} =& A_1 \cap A_2,\\
S_{01}^{11} =& A_1 \cap B_3,\\
S_{11}^{10} =& A_1 \cap A_4 \cap B_5,\\
S_{00}^{01} =& A_1 \cap A_3 \cap A_6,\\
S_{10}^{10} =& ((B_5 \cap A_7) \cup (A_5 \cap B_7)) \cap\\
& ((B_5 \cap A_2) \cup (A_5 \cap B_2)) \cap\\
& ((B_5 \cap A_1) \cup (A_5 \cap B_1)).
\end{aligned}$$

$$\begin{aligned}
\overline{S_{01}^{10}} =& A_1,\\
\overline{S_{10}^{00}} =& B_1 \cup B_2,\\
\overline{S_{01}^{11}} =& B_1 \cup A_3,\\
\overline{S_{11}^{10}} =& B_1 \cup B_4 \cup A_5,\\
\overline{S_{00}^{01}} =& B_1 \cup B_3 \cup B_6,\\
\overline{S_{10}^{10}} =& ((A_5 \cup B_7) \cap (B_5 \cup A_7)) \cup\\
& ((A_5 \cup B_2) \cap (B_5 \cup A_2)) \cup\\
& ((A_5 \cup B_1) \cap (B_5 \cup A_1)).
\end{aligned}$$

Ako je uvedené v (1.13), je množina T^* prienikom týchto množín $\overline{S_{ij}^{rs}}$. Platí

$$\begin{aligned}
T^* =& A_1 \cap B_2 \cap A_3 \cap (B_4 \cup A_5) \cap B_6 \cap (((A_5 \cup B_7) \cap (B_5 \cup A_7)) \cup\\
& ((A_5 \cup B_2) \cap (B_5 \cup A_2)) \cup ((A_5 \cup B_1) \cap (B_5 \cup A_1))).
\end{aligned}$$

Ďalej využijeme vzťah (4.2) na strane 52, ktorý nám dáva

$$\begin{aligned}T^* =& A_1 \cap B_2 \cap A_3 \cap (B_4 \cup A_5) \cap B_6 \cap ((A_5 \cap A_7) \cup (B_5 \cap B_7) \cup \\ & (A_5 \cap A_2) \cup (B_5 \cap B_2) \cup (A_5 \cap A_1) \cup (B_5 \cap B_1)) \\ =& A_1 \cap B_2 \cap A_3 \cap (B_4 \cup A_5) \cap B_6 \cap ((A_5 \cap A_7) \cup (B_5 \cap B_7) \cup B_5 \cup A_5) \\ =& A_1 \cap B_2 \cap A_3 \cap (B_4 \cup A_5) \cap B_6.\end{aligned}$$

Nakoniec využijeme, že $B_4 \cup A_5 = (A_4 \cap A_5) \cup (B_4 \cap B_5) \cup (B_4 \cap A_5)$ je zjednotenie disjunktných množín.

Celkovo teda môžeme množinu T^* zapísať ako zjednotenie 3 disjunktných množín, kde pre každú z týchto množín musíme kvôli asymptotickým odhadom pridať ešte podmienku $\chi(x) = \chi(2-x) = 1$ čo je ekvivalentné tomu, že do prieniku množín u každej z 3 disjunktných množín pridáme množiny A_8 a A_9. Preto sú všetky tieto disjunktné množiny, ktorých zjednotenie dáva T^*, dané 8 polynómami $p_1(x), p_2(x), p_3(x), p_4(x), p_5(x), p_6(x), p_8(x), p_9(x)$, ktorých súčet stupňov je 12. Zoznam všetkých disjunktných množín je uvedený v Tabuľke A.9, ktorá sa nachádza v prílohe tejto práce.

Môžeme pristúpiť k asymptotického odhadu veľkosti T^*, ktorý uvedieme v nasledujúcom tvrdení.

Tvrdenie 4.6. *Predpokladajme $q \equiv 3 \bmod 8$. Pre náhodne zvolené $(a,b) \in \Sigma$ také, že $(a,b) = \Psi^{-1}((x,y))$, kde x a y spĺňajú: $(x,y) \in S$ a $g_1(x,y) = 0$, je $Q_{a,b}$ maximálne neasociatívna kvázigrupa s pravdepodobnosťou $\approx 0{,}047$. Navyše platí, že maximálne neasociatívna kvázigrupa $Q_{a,b}$ spĺňajúca tieto podmienky vždy existuje pre $q > 413\,431$ a pre prvočíselné $q \leq 413\,431$ taká kvázigrupa existuje práve vtedy, keď $q \geq 19$ a zároveň $q \notin \{67, 83\}$.*

Dôkaz. Začneme odhadom asymptotickej veľkosti množiny T^*. Z diskusie pred týmto tvrdením plynie, že množinu T^* vieme zapísať ako zjednotenie 3 navzájom disjunktných množín. Preto Vetu 1.6 aplikujeme na každú z týchto množín samostatne a jednotlivé odhady sčítame.

Najprv overíme, že sú splnené predpoklady Vety 1.6. Polynómy, ktoré budeme vo vete využívať, sú $p_1(x), p_2(x), p_3(x), p_4(x), p_5(x), p_6(x), p_8(x), p_9(x)$. Z Lemma 4.3 plynie, že sa jedná o bezštvorcový zoznam polynómov, čím je predpoklad vety splnený.

V zozname týchto polynómov môže byť maximálne 12 rôznych koreňov. Keďže nás zaujíma asymptotický odhad, môžeme týchto niekoľko hodnôt x zanedbať. Preto pridaním členu s hodnotou 12 do nášho odhadu môžeme ďalej predpokladať, že x nie je koreňom žiadneho z týchto polynómov.

Teraz už môžeme aplikovať Vetu 1.6 a dostávame

$$\begin{aligned}\left||T^*| - 3 \cdot 2^{-8} q\right| &< (\sqrt{q}+1)(3 \cdot 12)/2 + 12, \\ \left||T^*| - 3 \cdot 2^{-8} q\right| &< (\sqrt{q}+1)18 + 12. \end{aligned} \tag{4.6}$$

Z toho je vidno, že

$$\lim_{q \to \infty} \frac{|T^*|}{q} \doteq 0{,}0117.$$

Opäť $\left|S'\right| \approx (q-1)/4$. V spojení s asymptotickým odhadom veľkosti množiny T^* je hľadaná pravdepodobnosť približne 0,047.

Využijeme vzťah (4.6) a dostávame, že maximálne neasociatívna kvázigrupa $Q_{a,b}$ existuje, ak platí

$$3 \cdot 2^{-8} q > (\sqrt{q} + 1)18 + 12.$$

To platí práve vtedy, keď $q > 2\,364\,413$. Aj v tomto prípade, sa dá táto hodnota znížiť tak, že ako podmnožinu T^* si vezmeme množinu $U = A_1 \cap B_2 \cap A_3 \cap B_4 \cap B_6 \cap A_8 \cap A_9$, ktorá je daná 7 polynómami so súčtom stupňov 10. Na zoznam tých polynómov aplikujeme Vetu 1.6 a dostávame, že pre $(x, y) \in U$ existuje maximálne neasociatívna kvázigrupa $Q_{a,b}$ práve vtedy, keď

$$2^{-7} q > (\sqrt{q} + 1)5 + 10,$$

čo platí práve vtedy, keď $q > 413\,431$. Zrejme teda platí, že pre $q > 413\,431$ taká kvázigrupa existuje pre $(x, y) \in T^*$.

Pre prvočíselné $q \leq 413\,431$ sme experimentálne overili, že taká kvázigrupa existuje práve vtedy, keď $q \geq 19$ a zároveň $q \notin \{67, 83\}$.

□

Rovnako aj v tomto prípade sme pravdepodobnosť uvedenú v predchádzajúcom tvrdení dodatočne experimentálne overili výpočtom skutočnej veľkosti množiny T^*. V tomto prípade je výsledok tohto overenia uvedený v grafe, ktorý je uvedený na Obrázku B.9 v prílohe tejto práce. Experimentálne overenie zrejme naznačuje správnosť našich výpočtov.

Na experimentálne overenie existencie maximálne neasociatívnej kvázigrupy na záver dôkazu Tvrdenia 4.6 sme opäť využili Algoritmus 7.

4.3.4 $q \equiv 7 \bmod 8$

Tentokrát budeme predpokladať $q \equiv 7 \bmod 8$. Tento prípad je takmer identický s prípadom $q \equiv 3 \bmod 8$ v sekcii 4.3.3, od ktorého sa líši len v podmienke pre množinu S_{10}^{10} ako je vidno v Lemma 4.2. Nebudeme preto tomuto prípadu venovať veľa pozornosti, ale uvedieme len dôležité informácie k určeniu hľadanej pravdepodobnosti.

V tomto prípade teda využívame rovnaké polynómy ako v sekcii 4.3.3 a preto aj množiny A_e a B_e budú totožné s predchádzajúcim prípadom. Podmienky pre množiny S_{ij}^{rs} majú tvar

$$\begin{aligned}
S_{01}^{10} =& B_1, \\
S_{10}^{00} =& A_1 \cap A_2, \\
S_{01}^{11} =& A_1 \cap B_3, \\
S_{11}^{10} =& A_1 \cap A_4 \cap B_5, \\
S_{00}^{01} =& A_1 \cap A_3 \cap A_6, \\
S_{10}^{10} =& ((B_5 \cap A_7) \cup (A_5 \cap B_7)) \cap \\
& ((B_5 \cap A_2) \cup (A_5 \cap B_2)) \cap \\
& ((A_5 \cap A_1) \cup (B_5 \cap B_1)).
\end{aligned}$$

Opäť postupujeme ako v obecnom prípade uvedenom v sekcii 1.4. Keďže je ďalší postup takmer identický s postupom v sekcii 4.3.3 uvedieme len zápis množiny T^* pomocou množín A_e a B_e, a potom transformáciu tohto zápisu na zjednotenie disjunktných množín. Platí teda

$$T^* = A_1 \cap B_2 \cap A_3 \cap (B_4 \cup A_5) \cap B_6 \cap ((A_5 \cap A_7) \cup B_5).$$

Využijeme, že $B_4 \cup A_5 = (A_4 \cap A_5) \cup (B_4 \cap B_5) \cup (B_4 \cap A_5)$ je zjednotenie disjunktných množín, čo nám dáva

$$(B_4 \cup A_5) \cap ((A_5 \cap A_7) \cup B_5) = (A_4 \cap A_5 \cap A_7) \cup (B_4 \cap B_5) \cup (B_4 \cap A_5 \cap A_7).$$

Celkovo teda môžeme množinu T^* zapísať ako zjednotenie 3 disjunktných množín, kde pre každú z týchto množín pridáme ešte prienik s A_8 a A_9. Preto 2 z týchto disjunktných množín sú dané 9 polynómami $p_1(x), \ldots, p_9(x)$ so súčtom stupňov 14 a zostávajúca množina je daná 8 polynómami $p_1(x), p_2(x), p_3(x)$, $p_4(x), p_5(x), p_6(x), p_8(x), p_9(x)$ so súčtom stupňov 12, čo nám k asymptotickým odhadom stačí. Zoznam disjunktných množín je uvedený v Tabuľke A.10, ktorá sa nachádza v prílohe tejto práce.

Môžeme pristúpiť k asymptotického odhadu veľkosti T^*, ktorý uvedieme v nasledujúcom tvrdení.

Tvrdenie 4.7. *Predpokladajme $q \equiv 7 \bmod 8$. Pre náhodne zvolené $(a, b) \in \Sigma$ také, že $(a, b) = \Psi^{-1}((x, y))$, kde x a y spĺňajú: $(x, y) \in S$ a $g_1(x, y) = 0$, je $Q_{a,b}$ maximálne neasociatívna kvázigrupa s pravdepodobnosťou $\approx 0{,}031$. Navyše platí, že maximálne neasociatívna kvázigrupa $Q_{a,b}$ spĺňajúca tieto podmienky vždy existuje pre $q > 2\,368\,503$ a pre prvočíselné $q \leq 2\,368\,503$ taká kvázigrupa existuje práve vtedy, keď $q \geq 71$ a zároveň $q \neq 431$.*

Dôkaz. Začneme odhadom asymptotickej veľkosti množiny T^*. Z diskusie pred týmto tvrdením plynie, že množinu T^* vieme zapísať ako zjednotenie 3 navzájom disjunktných množín. Preto Vetu 1.6 aplikujeme na každú z týchto množín samostatne a jednotlivé odhady sčítame.

Najprv overíme, že sú splnené predpoklady Vety 1.6. Polynómy, ktoré budeme vo vete využívať sú práve polynómy $p_1(x), \ldots, p_9(x)$. Z Lemma 4.3 plynie, že sa jedná o bezštvorcový zoznam polynómov, čím je predpoklad vety splnený.

V zozname týchto polynómov môže byť maximálne 14 rôznych koreňov. Keďže nás zaujíma asymptotický odhad, môžeme týchto niekoľko hodnôt x zanedbať. Preto pridaním členu s hodnotou 14 do nášho odhadu môžeme predpokladať, že x nie je koreňom žiadneho z týchto polynómov.

Teraz už môžeme aplikovať Vetu 1.6 a dostávame

$$\begin{aligned} \left||T^*| - (2 \cdot 2^{-9} + 2^{-8})q\right| &< (\sqrt{q} + 1)(2 \cdot 14 + 12)/2 + 14, \\ \left||T^*| - 2^{-7}q\right| &< (\sqrt{q} + 1)20 + 14. \end{aligned} \tag{4.7}$$

Z toho je vidno, že

$$\lim_{q \to \infty} \frac{|T^*|}{q} \doteq 0{,}0078.$$

Opäť $\left|S'\right| \approx (q-1)/4$. V spojení s asymptotickým odhadom veľkosti množiny T^* je hľadaná pravdepodobnosť približne 0,031.

Využijeme vzťah (4.7) a dostávame, že maximálne neasociatívna kvázigrupa $Q_{a,b}$ existuje, ak platí

$$2^{-7}q > (\sqrt{q}+1)20 + 14.$$

To platí práve vtedy, keď $q > 6\,562\,301$. Aj v tomto prípade, sa dá táto hodnota znížiť tak, že ako podmnožinu T^* si vezmeme množinu $U = A_1 \cap B_2 \cap A_3 \cap B_4 \cap B_5 \cap B_6 \cap A_8 \cap A_9$, ktorá je daná 8 polynómami so súčtom stupňov 12. Na zoznam tých polynómov aplikujeme Vetu 1.6 a dostávame, že pre $(x, y) \in U$ existuje maximálne neasociatívna kvázigrupa $Q_{a,b}$ práve vtedy, keď

$$2^{-8}q > (\sqrt{q}+1)6 + 12,$$

čo platí práve vtedy, keď $q > 2\,368\,503$. Zrejme teda platí, že pre $q > 2\,368\,503$ taká kvázigrupa existuje pre $(x, y) \in T^*$.

Pre prvočíselné $q \leq 2\,368\,503$ sme experimentálne overili, že taká kvázigrupa existuje práve vtedy, keď $q \geq 71$ a zároveň $q \neq 431$.

□

Rovnako aj v tomto prípade sme pravdepodobnosť uvedenú v predchádzajúcom tvrdení dodatočne experimentálne overili výpočtom skutočnej veľkosti množiny T^*. V tomto prípade je výsledok tohto overenia uvedený v grafe, ktorý je uvedený na Obrázku B.10 v prílohe tejto práce. Experimentálne overenie zrejme naznačuje správnosť našich výpočtov.

Na experimentálne overenie existencie maximálne neasociatívnej kvázigrupy na záver dôkazu Tvrdenia 4.7 sme opäť využili Algoritmus 7.

5. Implementácia výpočtov

Na overenie správnosti výpočtov a na uľahčenie práce, najmä pri hľadaní chýb počas písania práce, sme implementovali niekoľko jednoduchých algoritmov vychádzajúcich z teórie uvedenej v prvej kapitole tejto práce. V tejto časti by sme v stručnosti uviedli, čo presne sa nám podarilo implementovať a čo sa na základe toho podarilo spočítať.

Implementácia prebehla vo Wolfram Mathematica, verzia 12. Konkrétna implementácia je uvedená v elektronickej prílohe tejto práce. Tu uvedieme len popis jednotlivých algoritmov.

Prvým skriptom sa nám podarilo využitím vzťahu (1.13) získať pomocou množín S_{ij}^{rs} zápis množiny T^* ako booleovského výrazu v disjunktnej normálnej forme (DNF). Tento zápis množiny T^* sa ďalej využije v Algoritme 2.

Algoritmus 1: DNF

Vstup: Množiny S_{ij}^{rs} zapísané pomocou množín A_e a B_e, ktoré uvažujeme ako booleovský výraz;

Výstup: Množina T^* zapísaná v disjunktnej normálnej forme množinami A_e a B_e;

1 Každú množinu S_{ij}^{rs} zneguj ako booleovský výraz, čím získame tvar množiny $\overline{S_{ij}^{rs}}$;

2 Na zjednotenie množín $\overline{S_{ij}^{rs}}$ aplikuj funkciu na transformovanie booleovského výrazu na disjunktnú normálnu formu, to vráť na výstup;

Popis množiny T^*, vyplývajúci z disjunktnej normálnej formy množiny T^* uvažovanej ako booleovský výraz, je teda tvorený zjednotením niekoľkých množín. Tieto množiny sú dané prienikom vybraných množín A_e a B_e definovaných u konkrétneho prípadu, ktoré popisovali množiny S_{ij}^{rs} tak, ako sme to uviedli vo výpočtovej časti práce.

Nejde však o zjednotenie navzájom disjunktných množín. Je to len spôsob, akým zapísať množinu T^* tak, aby sme vedeli jednoducho získať podmienky, pomocou ktorých budeme testovať, či nejaká dvojica z S patrí do T^*. Napríklad u prípadu $t_1(x, y)$ pre $q \equiv 1 \bmod 8$ sme určili rozklad množiny T^* na zjednotenie 28 navzájom disjunktných množín, ale T^* v disjunktnej normálnej forme je tvorené zjednotením 6 množín. To nám ale nespôsobuje problém, pretože nám v tomto prípade nejde o asymptotický odhad, ale o test náležania do množiny.

Dodajme, že zápis množiny T^* ako zjednotenia navzájom disjunktných množín, ako sme ho uvádzali vo výpočtovej časti práce, nemá spojitosť s výstupom predchádzajúceho algoritmu. Vo výpočtovej časti sme vychádzali striktne zo zápisu množín S_{ij}^{rs} daného množinami A_e a B_e, a disjunktných rozklad sme odvodili bez pomoci implementovaného algoritmu. Dodajme, že napriek tomu je získaný disjunktný rozklad množiny T^* overený Algoritmom 5, ako ďalej vysvetlíme.

Druhým krokom pri týchto výpočtoch je využiť ďalší skript na transformáciu DNF na podmienky, ktoré nám umožnia testovať, či dvojica $(x, y) \in S$ patrí do T^*. To nám dovolí nasledujúci algoritmus, ktorý nám v konečnom dôsledku umožní pre dané q určiť počet dvojíc $(x, y) \in S'$, ktoré padnú do množiny T^*. Pripomeňme, že množina S' obsahuje tie dvojice $(x, y) \in S$, ktoré splňujú dodatočnú

podmienku medzi x a y danú jedným z polynómov $t_i(x, y)$.

Algoritmus 2: Podmienky na náležanie dvojice (x, y) do T^*

Vstup: $T^* = C_1 \cup \cdots \cup C_m$ ako výstup z Algoritmu 1;
Zoznam polynómov $p_1, \ldots, p_k$ v jednej neznámej, kde k je počet polynómov definovaných u konkrétneho prípadu. Polynómy zoradené tak, že p_e definuje množiny A_e a B_e;
Dodatočne pridané podmienky vyplývajúce z definície množiny S;

Výstup: Podmienky pre testovanie, či dvojica (x, y) patrí do T^*

1 **for** $i \leftarrow 0$ **to** m **do**

/* Dodatočné podmienky znamenajú podmienky, ktoré musí splniť dvojica (x, y), aby patrila do S, teda typicky také podmienky, aby x aj y boli rôzne nenulové štvorce rôzne od 1, kde ale jedna z neznámych je funkciou druhej neznámej */

2 Do prieniku množín A_e a B_e tvoriacich C_i pridaj dodatočné podmienky z definície S;

/* Na miesto $\chi()$ prakticky používame Jacobiho symbol, kde vkladáme daný polynóm a premennú q. Za q budeme neskôr nahradzovať skutočnú hodnotu q a do polynómu budeme dosadzovať testovacie hodnoty podľa konkrétneho prípadu. */

3 V C_i nahraď A_e výrazom $\chi(p_e) = 1$ pre každé $e \in \{1, \ldots, k\}$;

4 V C_i nahraď B_e výrazom $\chi(p_e) = -1$ pre každé $e \in \{1, \ldots, k\}$;

5 Prienik množín A_e a B_e v C_i nahraď logickou spojkou AND medzi výrazmi tvaru $\chi(p_e) = \pm 1$;

6 **end**

7 Pre $i \in \{1, \ldots, m\}$ spoj výrazy C_i do jedného logického výrazu pomocou logickej spojky OR a vráť na výstup;

Výsledkom predchádzajúceho algoritmu je teda logický výraz daný podmienkami využívajúcimi Jacobiho symbol pre prvočísla, ktorý ponúka jazyk Wolfram Mathematica na miesto Legendrov symbol. Ten je pre prvočíslo p a $a \in \mathbb{F}_p$ podobne ako kvadratický charakter definovaný tak, že pre dvojicu (a, p) vráti 1, ak existuje $b \in \mathbb{F}_p$, že $a \equiv b^2 \bmod p$, 0 ak je $a = 0$ a inak vráti -1.

Do tohto výrazu teda stačí dosadiť za q a v závislosti na tom, v akej neznámej vstupujú do výpočtov dané polynómy, nahradíme aj neznámu v polynómoch. Po dosadení teda vyhodnotíme pravdivosť výrazu. Ak sú dané podmienky splnené tak testovaná dvojica (x, y) pre dané q patrí do množiny T^*, v opačnom prípade tam nepatrí.

Pre overenie správnosti popisu T^* vytvoreného z množín S_{ij}^{rs} sme implementovali porovnanie, kde sme zrovnávali či dvojica (x, y) padne do T^* práve vtedy, keď je kvázigrupa $Q_{a,b}$ maximálne neasociatívna, kde $(a, b) = \Psi^{-1}((x, y))$, čo je dané vzťahom (1.7). Tento Algoritmus 5 využíva 2 ďalšie algoritmy, ktoré uvedieme pred týmto algoritmom. Ide o Algoritmus 3, ktorý pre $(x, y) \in S$ za daných dodatočných podmienok určí, či je kvázigrupa $Q_{a,b}$ maximálne neasociatívna pomocou rovnice asociativity. Druhým je Algoritmus 4, ktorý vytvorí zoznam dvojíc (x, y), ktoré tvoria množinu S'.

Algoritmus 3: Je kvázigrupa $Q_{a,b}$ maximálne neasociatívna?

Vstup: Dvojica $(x, y) \in S$
Charakteristika telesa q;
Výstup: True, ak je $Q_{a,b}$ maximálne neasociatívna, inak False;

```
/* Pre určenie hodnoty a a b využívame vzťah vo Vete (1.17).          */
```

1 $a := \frac{x(1-y)}{x-y}$;
2 $b := \frac{1-y}{x-y}$;
3 $R := \{(u, v) \in \mathbb{F}_q \times \mathbb{F}_q\}$;
4 JeMaxNeasoc := True;
5 **for** $(u, v) \in R$ **do**
6 Dosaď do rovnice asociativity dvojicu (u, v), kde kvadratický ortomorfizmus je daný hodnotou a a b;

```
/* Pripomeňme, že vďaka Vete 1.18 je kvázigrupa Q_{a,b} maximálne
   neasociatívna práve vtedy, keď jediným riešenim rovnice
   asociativity je dvojica (0,0).                                     */
```

7 **if** (u, v) *je riešenie rovnice asociativity a zároveň* $(u, v) \neq (0, 0)$ **then**
8 JeMaxNeasoc := False;
9 Break;
10 **end**
11 **end**
12 **return** JeMaxNeasoc;

Algoritmus 4: Množina S'

Vstup: Polynóm $p(x, y)$ určujúci vzťah medzi x a y;
Neznáma, za ktorú budeme do $p(x, y)$ dosadzovať;
Charakteristika telesa q;
Výstup: Množina S', ktorú tvoria dvojice $(x, y) \in S$ spĺňujúce $p(x, y) = 0$;

```
/* Na vstupe musíme určiť, za ktorú neznámu chceme do rovnice
   dosadzovať, pretože dosadzovaná neznáma sa pre rôzne prípady líši.
   */
```

1 $S' := \emptyset$;
2 $R := \{v \in \mathbb{F}_q : \chi(v) = 1, v \neq 1\}$;
3 **for** $v \in R$ **do**
4 Za neznámu, ktorá je na vstupe, dosaď do rovnice $p(x, y) = 0$ hodnotu v a dopočítaj hodnotu druhej neznámej, ktorú vlož do u;

```
/* u musí splniť nasledujúce podmienky, aby platilo (u,v) ∈ S.        */
```

5 **if** $u \neq 1$ *a* $u \neq 0$ *a* $u \neq v$ **then**
6 Podľa toho, za akú neznámu sme do rovnice dosadzovali pridaj buď dvojicu (u, v) alebo (v, u) do množiny S';
7 **end**
8 **end**
9 Vráť na výstup množinu S';

Teraz uvedieme algoritmus, ktorý nám umožní skontrolovať správnosť popisu množiny T^*, využitím dvoch predchádzajúcich algoritmov.

Algoritmus 5: Kontrola popisu množiny T^*

Vstup: Podmienky B pre testovanie, či dvojica (x, y) patrí do T^* ako výstup z Algoritmu 2;
Polynóm $p(x, y)$ určujúci vzťah medzi x a y;
Neznáma, za ktorú budeme do $p(x, y)$ dosadzovať;
Charakteristika telesa q;

Výstup: True, ak (x, y) patrí do T^* práve vtedy, keď $Q_{a,b}$ je maximálne neasociatívna kvázigrupa, inak False;

```
1 S' := Algoritmus 4 aplikovaný na p(x,y), neznámu zo vstupu, za ktorú
    dosadzujeme, a q;
2 for (x,y) ∈ S' do
      /* Pre prípad f_1(x,y) = 0, ktorý sme rozobrali v Kapitole 3 musí byť
         dvojica z množiny S' transformovaná na dvojicu (x,y). tak ako je
         to v danej kapitole vysvetlené, pretože množina S' v tomto
         prípade obsahuje dvojice (d,h) a tento algoritmus pre danú
         situáciu obsahuje ešte prevod na (x,y).                          */
3     Dosaď do podmienok B hodnotu q a podľa toho, za akú neznámu sme
        dosadzovali do rovnice pri určení množiny S', dosaď príslušnú
        hodnotu do polynómov v podmienkach B. Vyhodnoť výraz a ulož
        výsledok do α;
4     Aplikuj Algoritmus 3 na (x,y) a q a jeho výsledok ulož do β;
      /* Ak tieto dve hodnoty nie sú zhodné, je zrejmé, že získaný popis
         množiny T* nie je správny.                                       */
5     if α ≠ β then
6         return False;
7     end
8 end
9 return True;
```

V reálnej implementácií teda postupujeme tak, že si vytvoríme zoznam prvočísel v nejakom rozsahu $qMin$ a $qMax$, ktoré navyše splňujú $q \equiv \lambda \bmod \xi$, kde hodnoty λ a ξ sa líšia pre jednotlivé prípady, ktoré skúmame. Pre tento zoznam prvočísel teda v cykle voláme Algoritmus 5, čím sa nám pre každú situáciu podarilo overiť, že popis množiny T^* je v tomto zmysle správny a to pre prvočísla do veľkosti 800. Navyše bol tento algoritmus veľmi užitočný pri identifikovaní chyby počas hľadania správneho popisu množiny T^*, kde sa prípadna chyba prejavila už pri malých prvočíslach.

Ďalším automatizovaným výpočtom bola skutočná veľkosť množiny T^*. Ako vyplýva z výsledkov Algoritmu 5, je to zároveň počet maximálne neasociatívnych kvázigrup pre dané q, ktoré splňujú všetky dodatočné podmienky, ktoré kladieme v tejto práci na dvojicu (x, y). Tento výpočet sme vykonali pre prvočísla až do veľkosti 100 000 pre každú z 10 situácií, pre ktoré sme určili asymptotický odhad veľkosti množiny T^*. Využili sme k tomu už implementovaný Algoritmus 2, ktorý nám poskytuje podmienky na overenie, či $(x, y) \in T^*$ a tiež Algoritmus 4 pre získanie množiny S'. Cieľom tohto algoritmu je teda zistiť, či sa s rastúcim q blížime k hodnote, ktorú sme získali pomocou asymptotického odhadu veľkosti T^*. Z grafov uvedených v prílohe tejto práce, ktoré zobrazujú namerané dáta je zrejmé, že sa experimentálne overené výsledky blížia k hodnotám získaných

asymptotickými odhadmi pre každú z uvažovaných situácií.

Algoritmus 6: Skutočná veľkosť množiny T^*

Vstup: Podmienky B pre testovanie, či dvojica (x, y) patrí do T^* ako výstup z Algoritmu 2;
Polynóm $p(x, y)$ určujúci vzťah medzi x a y;
Neznáma, za ktorú budeme do $p(x, y)$ dosadzovať;
Rozsah $qMin$ a $qMax$, z ktorého vyberáme prvočísla splňujúce $q \equiv \lambda \bmod \xi$;

Výstup: Pre každé získané prvočíslo vráti počet $(x, y) \in S'$, pre ktoré platí $(x, y) \in T^*$, a tiež veľkosť S';

```
1  V := ∅;
2  Q := {q ∈ {qMin, ..., qMax} : q je prvočíslo > 2, q ≡ λ mod ξ};
3  for q ∈ Q do
4  |   c := 0;
5  |   S' := Algoritmus 4 aplikovaný na p(x, y), neznámu zo vstupu, za
   |    ktorú dosadzujeme, a q;
6  |   for (x, y) ∈ S' do
7  |   |   Dosaď do podmienok B hodnotu q a podľa toho, za akú neznámu
   |   |    sme dosadzovali do rovnice pri určení množiny S', dosaď
   |   |    príslušnú hodnotu do polynómov v podmienkach B. Vyhodnoť
   |   |    výraz a výsledok ulož do α;
8  |   |   if α = True then
9  |   |   |   c := c + 1;
10 |   |   end
11 |   end
12 |   Vlož do V trojicu (q, s, c), kde s je veľkosť S';
13 end
14 return V;
```

Posledným implementovaným skriptom je určenie, či pre dané prvočíselné q existuje aspoň jedna maximálne neasociatívna kvázigrupa $Q_{a,b}$. Tento výpočet prebieha podobne ako predchádzajúce a to tak, že pre zvolené q testujeme, či aspoň jedna dvojica (x, y) z S' patrí do T. Pre všetky skúmané prípady sa nám týmto výpočtom podarilo experimentálne overiť, že pre prvočíselné q taká maximálne neasociatívna kvázigrupa existuje aj pre menšie hodnoty q, než len tie, ktoré sme získali pomocou asymptotického odhadu.

Algoritmus 7: Existencia maximálne neasociatívnej kvázigrupy $Q_{a,b}$ príslušného rádu

Vstup: Podmienky B pre testovanie, či dvojica (x, y) patrí do T^* ako výstup z Algoritmu 2;
Polynóm $p(x, y)$ určujúci vzťah medzi x a y;
Neznáma, za ktorú budeme do $p(x, y)$ dosadzovať;
Rozsah $qMin$ a $qMax$, z ktorého vyberáme prvočísla splňujúce $q \equiv \lambda \bmod \xi$;

Výstup: Pre každé získané prvočíslo vráti True, ak existuje maximálne neasociatívna kvázigrupa $Q_{a,b}$ daného rádu, inak vráti False;

```
1  V := ∅;
2  Q := {q ∈ {qMin, ..., qMax} : q je prvočíslo > 1, q ≡ λ mod ξ};
3  for q ∈ Q do
4      exists := False;
5      R := {v ∈ F_q : χ(v) = 1, v ≠ 1};
6      for v ∈ R do
           /* V tomto prípade kvôli zrýchleniu výpočtu nevytvárame celú
              množinu S', ale hodnoty z tejto množiny priebežne testujeme,
              kým nenarazíme na prvú hodnotu, ktorá vyhovuje podmienkam.  */
7          Za neznámu, ktorá je na vstupe, dosaď do rovnice p(x, y) = 0
            hodnotu v a dopočítaj hodnotu druhej neznámej, ktorú vlož do u;
8          if u ≠ 1 a u ≠ 0 a u ≠ v then
9              Dosaď do podmienok B hodnotu q a tiež dosaď hodnotu v do
                polynómov v podmienkach B a vyhodnoť hodnotu výrazu,
                ktorú ulož do α;
10             if α = True then
11                 exists := True;
12                 Break;
13             end
14         end
15     end
16     Vlož do V dvojicu (q, exists)
17 end
18 return V;
```

Záver

Na záver nám ostáva zhrnúť dosiahnuté výsledky. Uveďme teda tieto výsledky v prehľadovej tabuľke.

	$t_1(x,y)=0$	$f_1(x,y)=0$	$g_1(x,y)=0$
$q \equiv 1 \bmod 8$	0,109	0,109	0,156
$q \equiv 5 \bmod 8$	0,219		0,172
$q \equiv 3 \bmod 8$	0,031	0,082	0,047
$q \equiv 7 \bmod 8$	0,047		0,031

Tabuľka 5.1: Pravdepodobnosti, že pre náhodne zvolené $(a,b) \in \Sigma$ je $Q_{a,b}$ maximálne neasociatívna kvázigrupa za dodatočných podmienok

Pre porovnanie, v obecnom prípade uvedenom v článku [4] sú tieto pravdepodobnosti nasledovne. Pri náhodnej voľbe $(a,b) \in \Sigma$ bude kvázigrupa $Q_{a,b}$ maximálne neasociatívna s pravdepodobnosťou $\approx 0{,}116$ ak je $q \equiv 1 \bmod 4$, a ak je $q \equiv 3 \bmod 4$, tak je táto pravdepodobnosť $\approx 0{,}05$.

Na prvý pohľad je zrejmé, že pre $q \equiv 1 \bmod 4$ sú 3 hodnoty z 5 uvedených väčšie ako pravdepodobnosť v obecnom prípade, navyše zvyšné 2 hodnoty (0,109) sú takmer rovnaké ako v obecnom prípade.

Pre $q \equiv 3 \bmod 4$ je situácia podobná, pretože v tomto prípade je vyššia pravdepodobnosť než v obecnom prípade len ak $f_1(x,y)=0$, ale v prípade $t_1(x,y)=0$ pre $q \equiv 3 \bmod 8$ a tiež $g_1(x,y)=0$ pre $q \equiv 7 \bmod 8$ je práve naopak, daná pravdepodobnosť výrazne nižšia. Teda v 3 prípadoch sa daná pravdepodobnosť zásadne líši od pravdepodobnosti v článku [4]. Zostávajúce 2 hodnoty (0,047) sa opäť od pôvodného výsledku zásadne nelíšia.

Celkovo teda môžeme povedať, že náš predpoklad, ktorý predpokladal zásadný rozdiel v pravdepodobnostiach u špeciálnych prípadov oproti obecnému prípadu bol správny len z časti. O výrazne odlišnej pravdepodobnosti môžeme hovoriť v 6 z 10 spočítaných situácií, pričom najväčší rozdiel v pravdepodobnosti je u situácie $t_1(x,y) = 0$ pre $q \equiv 5 \bmod 8$, ktorá je takmer dvojnásobná oproti obecnému prípadu.

Okrem uvedených pravdepodobností je dôležitým výsledkom práce aj dôkaz existencie takej maximálne neasociatívnej kvázigrupy pre q od určitej hranice, ktorá sa v každej zo spomínaných prípadov líši, a bola určená pomocou asymptotického odhadu. Navyše tiež úspešné overenie existencie pre prvočíselné q menšie než spomínaná hranica.

Ďalej ako jeden z vedľajších výsledkov práce môžeme upozorniť na potvrdenie faktu, že bezštvorcovosť zoznamu polynómov vyžadovaná pri Weilovom odhade použitom vo Vete 1.6 je skutočne nutná. Asymptotický odhad v [4] je totiž totožný s prípadom, keď sa v Tvrdeniach 1.26 a 1.27 volí jedna z premenných (napríklad y) pevne tak, aby polynómy v jednej neznámej (napríklad v x), ktoré takto vzniknú, boli bezštvorcové a je vždy konečný počet hodnôt y, ktoré túto podmienku porušujú. Predmetom skúmania tejto práce boli práve tie situácie,

kedy bolo y položené jednej z tých hodnôt, ktorá narušovala bezštvorcovosť zoznamu polynómov. Výsledky ukazujú, že sa za týchto okolností asymptotická pravdepodobnosť u väčšiny prípadov líši od tej platnej v prípade dosadenia jednej premennej a získania bezštvorcového zoznamu.

Zrejme sú v prípade $t_1(x, y) = 0$ pre $q \equiv 7 \bmod 8$ a tiež v prípade $g_1(x, y) = 0$ pre $q \equiv 3 \bmod 8$ uvedené pravdepodobnosti rovnaké. Rovnako to platí aj pre $t_1(x, y) = 0$ pre $q \equiv 3 \bmod 8$ a $g_1(x, y) = 0$ pre $q \equiv 7 \bmod 8$. Je teda možné, že sa pre tieto prípady, keď sa dané hodnoty zhodujú, dá nájsť jednotný popis, ktorý by tieto prípady umožnil riešiť ako jeden. Tento popis sa nám však nepodarilo objaviť, ale mohlo by to byť predmetom ďalšieho skúmania.

V úplnom závere teda môžeme zhodnotiť, že cieľ našej práce bol splnený. Podarilo sa nám preskúmať všetky špeciálne prípady, pre ktoré sme určili asymptotickú hustotu maximálne neasociativných kvázigrup a tiež sme dokázali ich existenciu za uvádzaných podmienok. Navyše sa nám to podarilo podporiť experimentálnym overením správnosti pre rozumne veľké prvočísla a tiež sa podarilo experimentálne overiť existenciu maximálne neasociatívnych kvázigrup pre menšie prvočísla, než pre ktoré bola existencia dokázaná pomocou asymptotického odhadu. Jednou z dôležitých častí práce bola potreba zápisu podmienok z Tvrdení 1.26 a 1.27 pomocou množín A_e a B_e, ktoré umožnili prehľadnejšie uvedenie jednotlivých prípadov a celkovú lepšiu prehľadnosť práce. Nakoniec stojí za spomenutie ešte prvá kapitola s teoretickou časťou práce, ktorá sa snažila čitateľovi priblížiť daný problém s dôrazom na podrobnejšie vysvetlenie problematiky, čo sa podľa nás podarilo.

Zoznam použitej literatúry

[1] Victor A. Shcherbacov, Quasigroups in cryptology, *Comput. Sci. J. Moldova* **17** (2009), no. 2, 193-228.

[2] Otokar Grošek and Peter Horák, On quasigroups with few associative triples, *Des. Codes Cryptogr.* **64** (2012), no. 1-2, 221-227.

[3] Aleš Drápal and Ian M. Wanless, Maximally nonassociative quasigroups via quadratic orthomorphisms, vyjde v *Algebraic Combinatorics*.

[4] Aleš Drápal and Ian M. Wanless, On the number of quadratic orthomorphisms that produce maximally nonassociative quasigroups, v recenznom riadení.

[5] Oskar Perron, Bemerkungen über die Verteilung der quadratischen Reste, (German) Math. Z. **56** (1952), 122-130.

[6] Gary L. Mullen and Daniel Panario, *Handbook of Finite Fields*, CRC Press, 2013.

[7] Petr Lisoněk, Maximal nonassociativity via fields, *Des. Codes Cryptogr.* **88** (2020), no. 12, 2521-2530.

[8] André Weil, On Some Exponential Sums, *Proc. Nat. Acad. Sci. U.S.A.* **34** (1948), 204-207.

[9] Anthony B. Evans, *Orthogonal Latin squares based on groups*, Developments in Mathematics **57**, Springer, Cham, 2018.

A. Tabuľky

i	$p_1(y)$	$p_2(y)$	$p_3(y)$	$p_4(y)$	$p_5(y)$	$p_6(y)$	$p_7(y)$	$p_8(y)$	$p_9(y)$	$p_{10}(y)$
1	−	+	−	−	−	+	+	+	+	+
2	−	−	+	−	−	+	+	+	+	+
3	−	+	+	−	−	+	+	+	+	+
4	−	+	−	−	+	+	+	+	+	+
5	−	+	−	−	−	+	+	−	+	+
6	−	−	+	−	−	+	+	−	+	+
7	−	+	+	−	−	+	+	−	+	+
8	−	+	−	−	+	+	+	−	+	+
9	−	+	−	−	−	+	−	+	+	+
10	−	−	+	−	−	+	−	+	+	+
11	−	+	+	−	−	+	−	+	+	+
12	−	+	−	−	+	+	−	+	+	+
13	−	+	−	−	−	+	−	−	+	+
14	−	−	+	−	−	+	−	−	+	+
15	−	+	+	−	−	+	−	−	+	+
16	−	+	−	−	+	+	−	−	+	+
17	−	+	−	−	−	−	+	+	+	+
18	−	−	+	−	−	−	+	+	+	+
19	−	+	+	−	−	−	+	+	+	+
20	−	+	−	−	+	−	+	+	+	+
21	−	+	−	−	−	−	+	−	+	+
22	−	−	+	−	−	−	+	−	+	+
23	−	+	+	−	−	−	+	−	+	+
24	−	+	−	−	+	−	+	−	+	+
25	−	+	−	−	−	−	−	−	+	+
26	−	−	+	−	−	−	−	−	+	+
27	−	+	+	−	−	−	−	−	+	+
28	−	+	−	−	+	−	−	−	+	+

Pozn: "+": $\chi(p_j(y)) = 1$ a "−": $\chi(p_j(y)) = -1$

Tabuľka A.1: Zoznam disjunktných množín, ktorých zjednotenie dáva T^*. Prípad $t_1(x, y) = 0$ pre $q \equiv 1 \bmod 8$ uvedený v sekcii 2.3.1

i	$p_1(y)$	$p_2(y)$	$p_3(y)$	$p_4(y)$	$p_5(y)$	$p_6(y)$	$p_7(y)$	$p_8(y)$	$p_9(y)$
1	−	+	−	−	+	+	+	+	+
2	−	−	+	−	+	+	+	+	+
3	−	+	+	−	+	+	+	+	+
4	−	+	−	+	+	+	+	+	+
5	−	+	−	−	−	−	+	+	+
6	−	−	+	−	−	−	+	+	+
7	−	+	+	−	−	−	+	+	+
8	−	+	−	+	−	−	+	+	+
9	−	+	−	−	+	−	+	+	+
10	−	−	+	−	+	−	+	+	+
11	−	+	+	−	+	−	+	+	+
12	−	+	−	+	+	−	+	+	+
13	−	+	−	−	+	−	−	+	+
14	−	−	+	−	+	−	−	+	+
15	−	+	+	−	+	−	−	+	+
16	−	+	−	+	+	−	−	+	+
17	−	+	−	−	−	+	+	+	+
18	−	−	+	−	−	+	+	+	+
19	−	+	+	−	−	+	+	+	+
20	−	+	−	+	−	+	+	+	+
21	−	+	−	−	−	+	−	+	+
22	−	−	+	−	−	+	−	+	+
23	−	+	+	−	−	+	−	+	+
24	−	+	−	+	−	+	−	+	+
25	−	+	−	−	−	−	−	+	+
26	−	−	+	−	−	−	−	+	+
27	−	+	+	−	−	−	−	+	+
28	−	+	−	+	−	−	−	+	+

Pozn: "+": $\chi(p_j(y)) = 1$ a "−": $\chi(p_j(y)) = -1$

Tabuľka A.2: Zoznam disjunktných množín, ktorých zjednotenie dáva T^*. Prípad $t_1(x, y) = 0$ pre $q \equiv 5 \bmod 8$ uvedený v sekcii 2.3.2

i	$p_1(y)$	$p_2(y)$	$p_3(y)$	$p_4(y)$	$p_5(y)$	$p_6(y)$	$p_7(y)$	$p_8(y)$	$p_9(y)$
1	+	+	+	−	−	0	0	+	+

Pozn: "+": $\chi(p_j(y)) = 1$, "−": $\chi(p_j(y)) = -1$ a "0": $p_j(y)$ nemá vplyv

Tabuľka A.3: Zoznam disjunktných množín, ktorých zjednotenie dáva T^*. Prípad $t_1(x, y) = 0$ pre $q \equiv 3 \bmod 8$ uvedený v sekcii 2.3.3

i	$p_1(y)$	$p_2(y)$	$p_3(y)$	$p_4(y)$	$p_5(y)$	$p_6(y)$	$p_7(y)$	$p_8(y)$
1	+	+	+	−	+	−	+	+
2	+	+	+	−	−	+	+	+
3	+	+	+	−	−	−	+	+

Pozn: "+": $\chi(p_j(y)) = 1$ a "−": $\chi(p_j(y)) = -1$

Tabuľka A.4: Zoznam disjunktných množín, ktorých zjednotenie dáva T^*. Prípad $t_1(x, y) = 0$ pre $q \equiv 7 \bmod 8$ uvedený v sekcii 2.3.4

i	$p_1(d)$	$p_2(d)$	$p_3(d)$	$p_4(d)$	$p_5(d)$	$p_6(d)$	$p_7(d)$	$p_8(d)$	$p_9(d)$	$p_{10}(d)$
1	−	−	−	−	−	−	−	+	+	+
2	−	+	+	−	−	−	−	+	+	+
3	−	−	+	−	−	−	−	+	+	+
4	−	−	−	−	+	−	−	+	+	+
5	−	−	−	−	−	+	+	−	+	+
6	−	+	+	−	−	+	+	−	+	+
7	−	−	+	−	−	+	+	−	+	+
8	−	−	−	−	+	+	+	−	+	+
9	−	−	−	−	−	+	−	+	+	+
10	−	+	+	−	−	+	−	+	+	+
11	−	−	+	−	−	+	−	+	+	+
12	−	−	−	−	+	+	−	+	+	+
13	−	−	−	−	−	+	−	−	+	+
14	−	+	+	−	−	+	−	−	+	+
15	−	−	+	−	−	+	−	−	+	+
16	−	−	−	−	+	+	−	−	+	+
17	−	−	−	−	−	−	+	+	+	+
18	−	+	+	−	−	−	+	+	+	+
19	−	−	+	−	−	−	+	+	+	+
20	−	−	−	−	+	−	+	+	+	+
21	−	−	−	−	−	−	+	−	+	+
22	−	+	+	−	−	−	+	−	+	+
23	−	−	+	−	−	−	+	−	+	+
24	−	−	−	−	+	−	+	−	+	+
25	−	−	−	−	−	+	+	+	+	+
26	−	+	+	−	−	+	+	+	+	+
27	−	−	+	−	−	+	+	+	+	+
28	−	−	−	−	+	+	+	+	+	+

Pozn: "+": $\chi(p_j(d)) = 1$ a "−": $\chi(p_j(d)) = -1$

Tabuľka A.5: Zoznam disjunktných množín, ktorých zjednotenie dáva T^*. Prípad $f_1(x, y) = 0$ pre $q \equiv 1 \bmod 4$ uvedený v sekcii 3.3.1

i	$p_1(d)$	$p_2(d)$	$p_3(d)$	$p_4(d)$	$p_5(d)$	$p_6(d)$	$p_7(d)$	$p_8(d)$	$p_9(d)$	$p_{10}(d)$
1	+	−	−	+	−	−	0	0	+	+
2	+	−	−	−	+	−	0	0	+	+
3	+	−	−	−	−	−	0	0	+	+
4	+	−	−	+	−	+	−	+	+	+
5	+	−	−	−	+	+	−	+	+	+
6	+	−	−	−	−	+	−	+	+	+
7	+	−	−	+	−	+	+	−	+	+
8	+	−	−	−	+	+	+	−	+	+
9	+	−	−	−	−	+	+	−	+	+
10	+	−	−	+	−	+	−	−	+	+
11	+	−	−	−	+	+	−	−	+	+
12	+	−	−	−	−	+	−	−	+	+

Pozn: "+": $\chi(p_j(d)) = 1$, "−": $\chi(p_j(d)) = -1$ a "0": $p_j(d)$ nemá vplyv

Tabuľka A.6: Zoznam disjunktných množín, ktorých zjednotenie dáva T^*. Prípad $f_1(x, y) = 0$ pre $q \equiv 3 \bmod 4$ uvedený v sekcii 3.3.2

i	$p_1(x)$	$p_2(x)$	$p_3(x)$	$p_4(x)$	$p_5(x)$	$p_6(x)$	$p_7(x)$	$p_8(x)$	$p_9(x)$	$p_{10}(x)$
1	−	−	−	+	−	−	0	0	+	+
2	−	+	+	+	−	−	0	0	+	+
3	−	−	+	+	−	−	0	0	+	+
4	−	−	−	+	−	+	0	0	+	+
5	−	−	−	−	+	−	+	−	+	+
6	−	+	+	−	+	−	+	−	+	+
7	−	−	+	−	+	−	+	−	+	+
8	−	−	−	−	+	+	+	−	+	+
9	−	−	−	−	−	−	+	−	+	+
10	−	+	+	−	−	−	+	−	+	+
11	−	−	+	−	−	−	+	−	+	+
12	−	−	−	−	−	+	+	−	+	+
13	−	−	−	−	+	−	−	+	+	+
14	−	+	+	−	+	−	−	+	+	+
15	−	−	+	−	+	−	−	+	+	+
16	−	−	−	−	+	+	−	+	+	+
17	−	−	−	−	−	−	−	+	+	+
18	−	+	+	−	−	−	−	+	+	+
19	−	−	+	−	−	−	−	+	+	+
20	−	−	−	−	−	+	−	+	+	+
21	−	−	−	−	+	−	−	−	+	+
22	−	+	+	−	+	−	−	−	+	+
23	−	−	+	−	+	−	−	−	+	+
24	−	−	−	−	+	+	−	−	+	+
25	−	−	−	−	−	−	−	−	+	+
26	−	+	+	−	−	−	−	−	+	+
27	−	−	+	−	−	−	−	−	+	+
28	−	−	−	−	−	+	−	−	+	+

Pozn: "+": $\chi(p_j(x)) = 1$, "−": $\chi(p_j(x)) = -1$ a "0": $p_j(x)$ nemá vplyv

Tabuľka A.7: Zoznam disjunktných množín, ktorých zjednotenie dáva T^*. Prípad $g_1(x, y) = 0$ pre $q \equiv 1 \bmod 8$ uvedený v sekcii 4.3.1

i	$p_1(x)$	$p_2(x)$	$p_3(x)$	$p_4(x)$	$p_5(x)$	$p_6(x)$	$p_7(x)$	$p_8(x)$	$p_9(x)$	$p_{10}(x)$
1	−	−	−	−	+	−	0	0	+	+
2	−	+	+	−	+	−	0	0	+	+
3	−	−	+	−	+	−	0	0	+	+
4	−	−	−	−	+	+	0	0	+	+
5	−	−	−	−	−	−	0	0	+	+
6	−	+	+	−	−	−	0	0	+	+
7	−	−	+	−	−	−	0	0	+	+
8	−	−	−	−	−	+	0	0	+	+
9	−	−	−	+	−	−	−	+	+	+
10	−	+	+	+	−	−	−	+	+	+
11	−	−	+	+	−	−	−	+	+	+
12	−	−	−	+	−	+	−	+	+	+
13	−	−	−	+	−	−	+	−	+	+
14	−	+	+	+	−	−	+	−	+	+
15	−	−	+	+	−	−	+	−	+	+
16	−	−	−	+	−	+	+	−	+	+
17	−	−	−	+	−	−	+	+	+	+
18	−	+	+	+	−	−	+	+	+	+
19	−	−	+	+	−	−	+	+	+	+
20	−	−	−	+	−	+	+	+	+	+

Pozn: "+": $\chi(p_j(x)) = 1$, "−": $\chi(p_j(x)) = -1$ a "0": $p_j(x)$ nemá vplyv

Tabuľka A.8: Zoznam disjunktných množín, ktorých zjednotenie dáva T^*. Prípad $g_1(x, y) = 0$ pre $q \equiv 5 \bmod 8$ uvedený v sekcii 4.3.2

i	$p_1(x)$	$p_2(x)$	$p_3(x)$	$p_4(x)$	$p_5(x)$	$p_6(x)$	$p_7(x)$	$p_8(x)$	$p_9(x)$
1	+	−	+	+	+	−	0	+	+
2	+	−	+	−	−	−	0	+	+
3	+	−	+	−	+	−	0	+	+

Pozn: "+": $\chi(p_j(x)) = 1$, "−": $\chi(p_j(x)) = -1$ a "0": $p_j(x)$ nemá vplyv

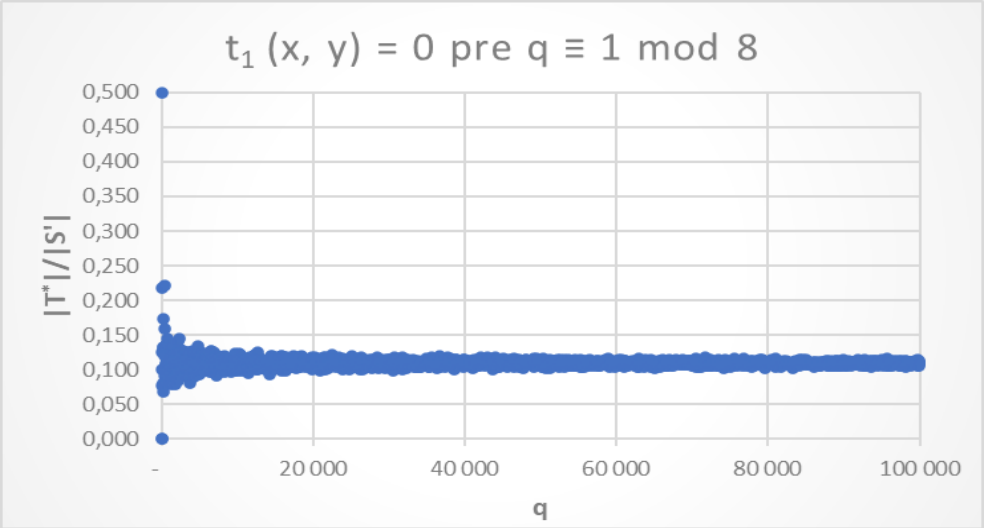
Tabuľka A.9: Zoznam disjunktných množín, ktorých zjednotenie dáva T^*. Prípad $g_1(x, y) = 0$ pre $q \equiv 3 \bmod 8$ uvedený v sekcii 4.3.3

i	$p_1(x)$	$p_2(x)$	$p_3(x)$	$p_4(x)$	$p_5(x)$	$p_6(x)$	$p_7(x)$	$p_8(x)$	$p_9(x)$
1	+	−	+	+	+	−	+	+	+
2	+	−	+	−	−	−	0	+	+
3	+	−	+	−	+	−	+	+	+

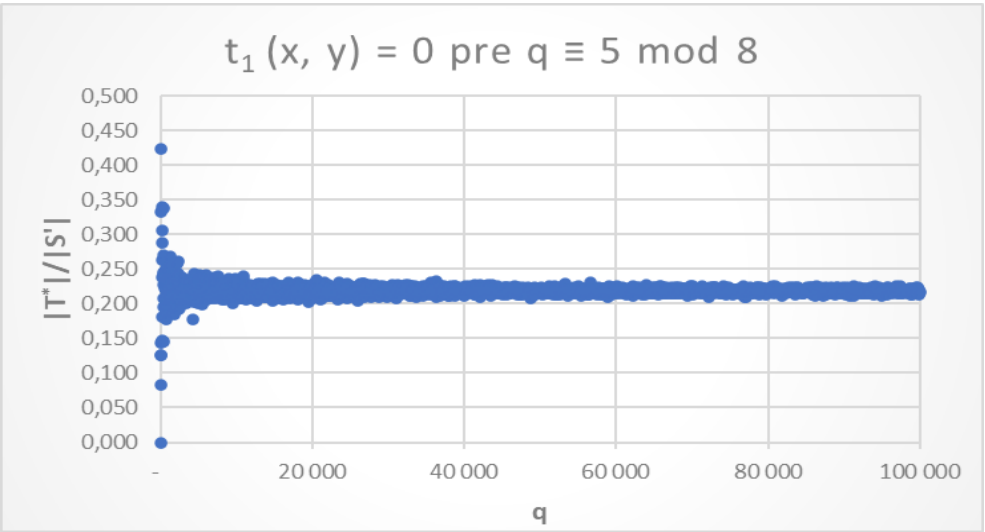
Pozn: "+": $\chi(p_j(x)) = 1$, "−": $\chi(p_j(x)) = -1$ a "0": $p_j(x)$ nemá vplyv

Tabuľka A.10: Zoznam disjunktných množín, ktorých zjednotenie dáva T^*. Prípad $g_1(x, y) = 0$ pre $q \equiv 7 \bmod 8$ uvedený v sekcii 4.3.4

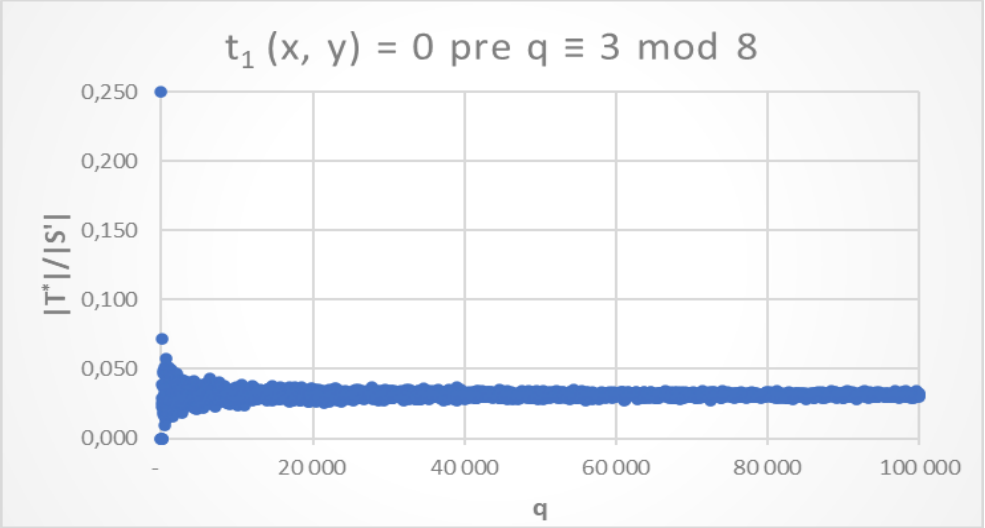
B. Grafy



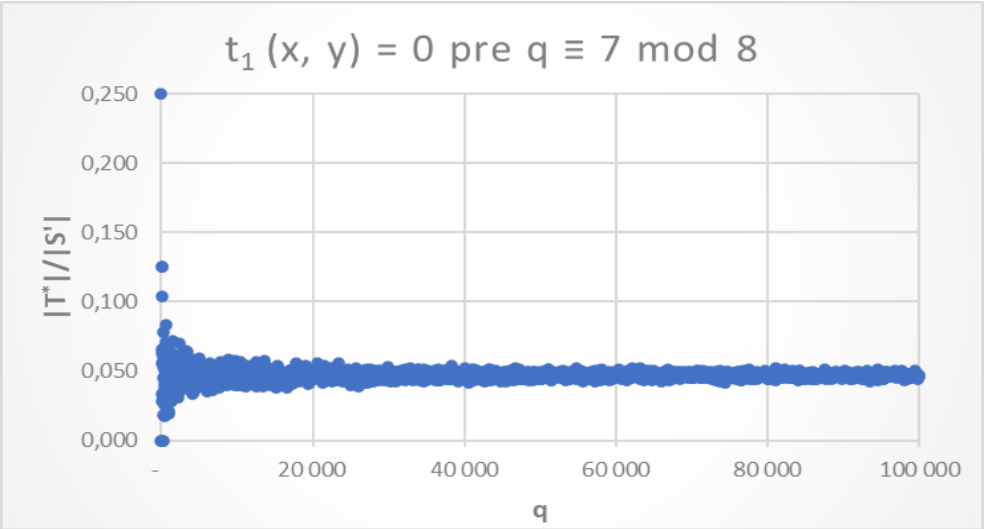
Obr. B.1: Pomer veľkosti množiny T^* k množine S' v prípade $t_1(x, y) = 0$ pre $q \equiv 1 \bmod 8$ uvedenom v sekcii 2.3.1



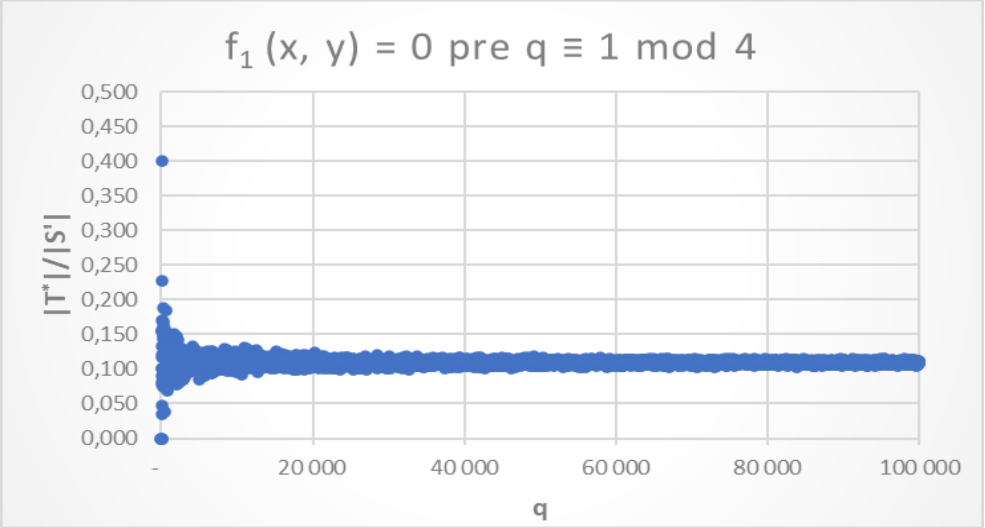
Obr. B.2: Pomer veľkosti množiny T^* k množine S' v prípade $t_1(x, y) = 0$ pre $q \equiv 5 \bmod 8$ uvedenom v sekcii 2.3.2



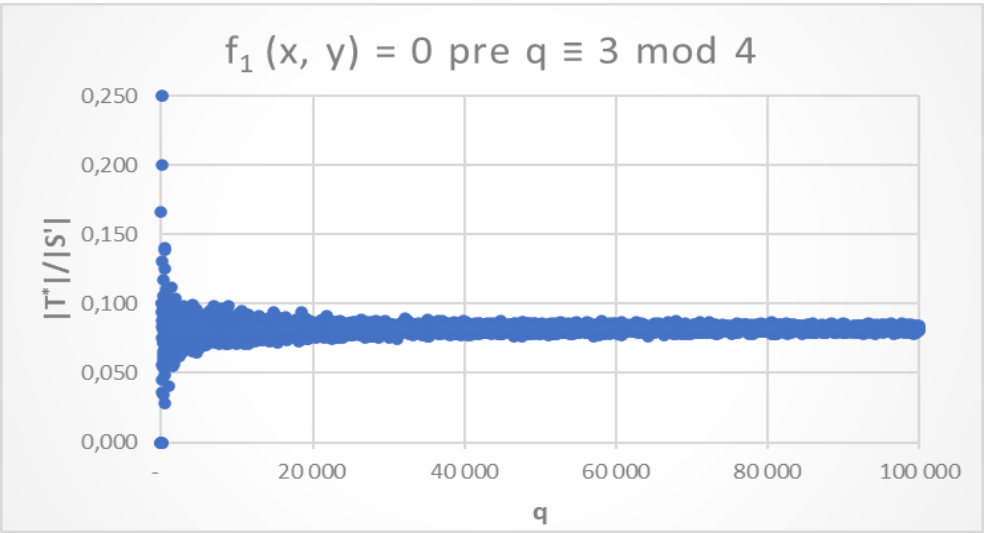
Obr. B.3: Pomer veľkosti množiny T^* k množine S' v prípade $t_1(x, y) = 0$ pre $q \equiv 3 \bmod 8$ uvedenom v sekcii 2.3.3



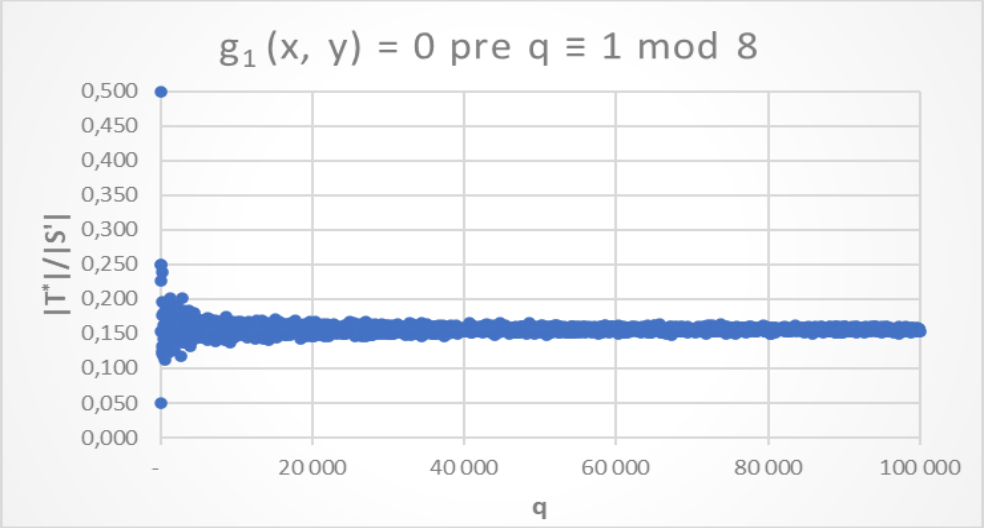
Obr. B.4: Pomer veľkosti množiny T^* k množine S' v prípade $t_1(x, y) = 0$ pre $q \equiv 7 \bmod 8$ uvedenom v sekcii 2.3.4



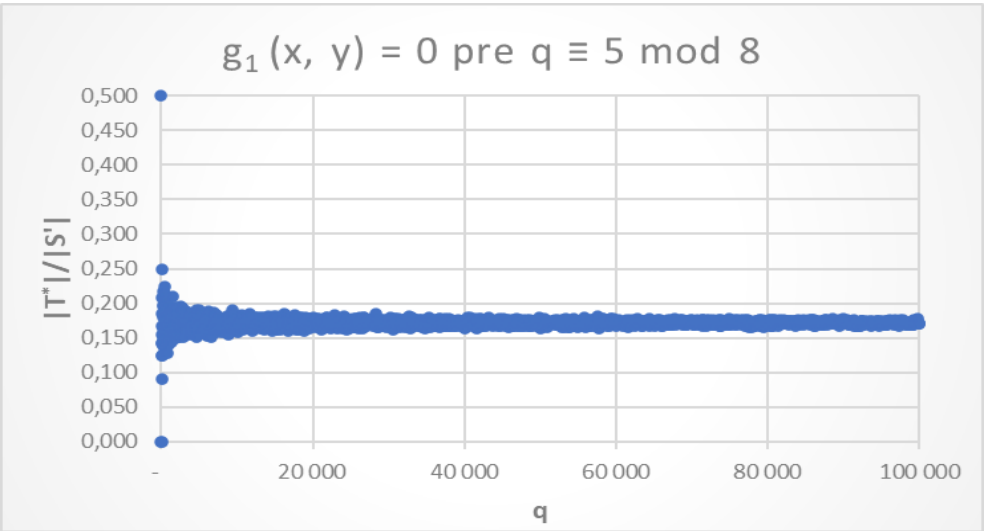
Obr. B.5: Pomer veľkosti množiny T^* k množine S' v prípade $f_1(x, y) = 0$ pre $q \equiv 1 \bmod 4$ uvedenom v sekcii 3.3.1



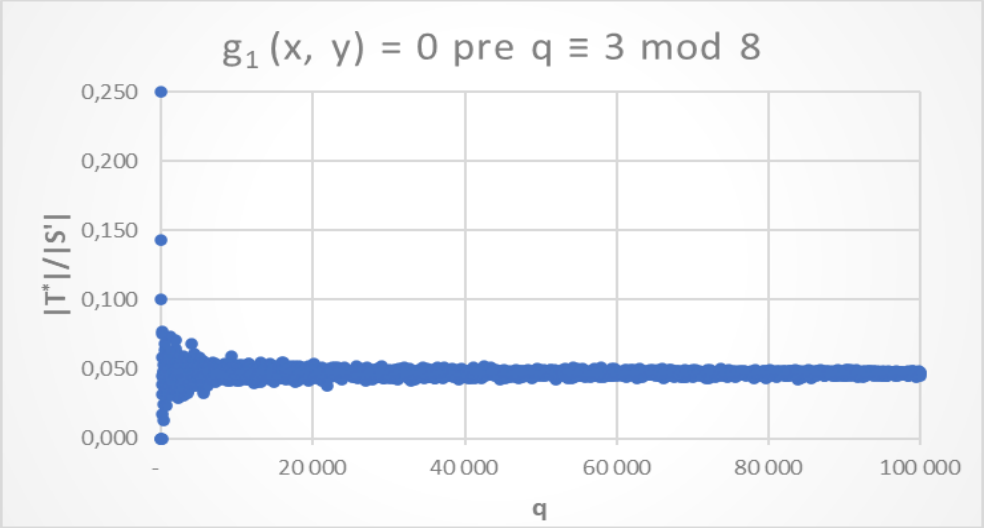
Obr. B.6: Pomer veľkosti množiny T^* k množine S' v prípade $f_1(x, y) = 0$ pre $q \equiv 3 \bmod 4$ uvedenom v sekcii 3.3.2



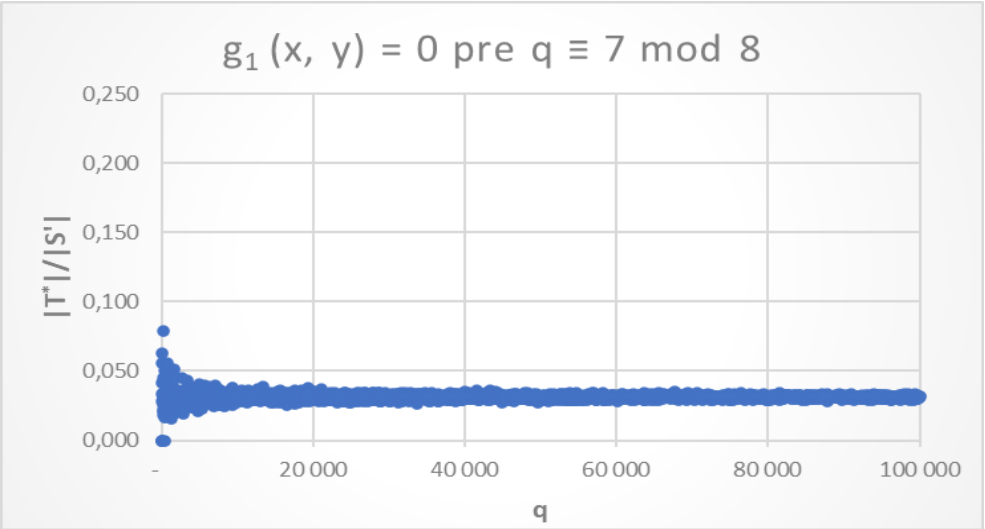
Obr. B.7: Pomer veľkosti množiny T^* k množine S' v prípade $g_1(x, y) = 0$ pre $q \equiv 1 \bmod 8$ uvedenom v sekcii 4.3.1



Obr. B.8: Pomer veľkosti množiny T^* k množine S' v prípade $g_1(x, y) = 0$ pre $q \equiv 5 \bmod 8$ uvedenom v sekcii 4.3.2



Obr. B.9: Pomer veľkosti množiny T^* k množine S' v prípade $g_1(x, y) = 0$ pre $q \equiv 3 \bmod 8$ uvedenom v sekcii 4.3.3



Obr. B.10: Pomer veľkosti množiny T^* k množine S' v prípade $g_1(x, y) = 0$ pre $q \equiv 7 \bmod 8$ uvedenom v sekcii 4.3.4